

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Takafumi UENO

Serial No. : Not Yet Assigned

Filed : Concurrently Herewith

For : TRANMISSION APPARATUS AND RECEIVING APPARATUS

CLAIM OF PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Applicant hereby claims the right of priority granted pursuant to 35 U.S.C. 119 based upon Japanese Application No. 2002-210727, filed July 19, 2002. As required by 37 C.F.R. 1.55, a certified copy of the Japanese application is being submitted herewith.

Respectfully submitted,
Takafumi UENO

*Leslie M. Danner Reg. No.
Bruce H. Bernstein 33,329*
Reg. No. 29,027

July 16, 2003
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: 2002年 7月19日

出願番号
Application Number: 特願2002-210727

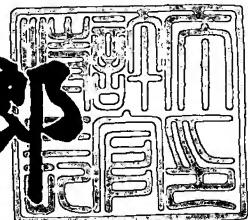
[ST.10/C]: [JP2002-210727]

出願人
Applicant(s): 松下電器産業株式会社

2003年 6月16日

特許庁長官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3046895

【書類名】 特許願

【整理番号】 2054041179

【提出日】 平成14年 7月19日

【あて先】 特許庁長官殿

【国際特許分類】 H04K 1/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 上野 孝文

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 送信装置、及び受信装置

【特許請求の範囲】

【請求項1】 データを暗号化して第1の暗号化データを生成する暗号化手段と、

第1の暗号化データと第1の暗号化データのプログラム番号との対応を示すテーブルを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、

第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを生成するツールリスト生成手段と、

前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、

第1の暗号化データに付随する権利情報を生成する権利情報生成手段と、

第1の暗号化データと前記プログラム仕様情報と前記ツールリストと前記制御グラフと前記権利情報を多重化する多重化手段とを有する送信装置。

【請求項2】 データを暗号化して第1の暗号化データを生成する暗号化手段と、

第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを生成するツールリスト生成手段と、

前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、

第1の暗号化データに付随する権利情報を生成する権利情報生成手段と、

第1の暗号化データと第1の暗号化データのプログラム番号との対応を示すテーブルと前記ツールリストと前記制御グラフと前記権利情報を含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、

第1の暗号化データと前記プログラム仕様情報を多重化する多重化手段とを有する送信装置。

【請求項3】 データを暗号化して第1の暗号化データを生成する暗号化手段と、

第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリ

ストを生成するツールリスト生成手段と、

前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御
グラフ生成手段と、

第1の暗号化データと第1の暗号化データのプログラム番号との対応を示すテ
ーブルと前記ツールリストと前記制御グラフと前記権利情報とを含むプログラム
仕様情報を生成するプログラム仕様情報生成手段と、

前記データに付隨する権利情報を生成する権利情報生成手段と、

前記権利情報を出力する権利情報送信手段と、

第1の暗号化データと前記プログラム仕様情報を多重化して出力する多重化
手段とを有する送信装置。

【請求項4】 前記権利情報と前記データとの対応付けを行う前記権利情報送
信手段を有する請求項3に記載の送信装置。

【請求項5】 前記権利情報と前記データとの対応付けを行う前記プログラム
仕様情報生成手段を有する請求項3に記載の送信装置。

【請求項6】 暗号を復号する復号ツールを多重化する前記多重化手段を有す
る請求項1乃至請求項5いずれかに記載の送信装置。

【請求項7】 暗号を復号するための鍵情報を多重化する前記多重化手段を有
する請求項1乃至請求項6いずれかに記載の送信装置。

【請求項8】 第1の暗号化データを含む多重化信号を少なくとも第1の暗号
化データとプログラム仕様情報とに分離する多重化分離手段と、

前記多重化信号から第1の暗号化データを復号する復号ツールを示すツールI
Dを有するツールリストを分離するツールリスト分離手段と、

前記多重化信号から前記復号ツールの受信装置での組み込み位置を示す制御
グラフを分離する制御グラフ分離手段と、

前記多重化信号から第1の暗号化データに付隨する権利情報を分離する権利情
報手段と、

前記ツールリストから取得したツールIDに従ってツールを入手し、前記制御
グラフに従って前記ツールを組み込む第1の制御手段と、

前記権利情報に従って第1の暗号化データを処理する第1の権利管理手段とを

有する受信装置。

【請求項9】 第1の暗号化データを含む多重化信号を少なくとも第1の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、

前記プログラム仕様情報から第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを分離するツールリスト分離手段と、

前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、

前記プログラム仕様情報から第1の暗号化データに付随する権利情報を分離する権利情報手段と、

前記ツールリストから取得したツールIDを有するツールを前記制御グラフに従って組み込む第1の制御手段と、

前記権利情報に従って第1の暗号化データを処理する第1の権利管理手段とを有する受信装置。

【請求項10】 第1の暗号化データを含む多重化信号を少なくとも第1の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、

前記プログラム仕様情報から第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを分離するツールリスト分離手段と、

前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、

前記ツールリストから取得したツールIDを有するツールを前記制御グラフに従って組み込む第1の制御手段と、

第1の暗号化データに付随する権利情報を受信する権利情報受信手段と、

前記権利情報に従って第1の暗号化データを処理する第1の権利管理手段とを有する受信装置。

【請求項11】 受信した第1の暗号化データを一時的に記憶する一時記憶手段と、

前記一時記憶手段に記憶された第1の暗号化データを読み取る読み取り手段を有する請求項8乃至請求項10いずれかに記載の受信装置。

【請求項12】 前記権利情報に記述された再生許諾が満了した後に第1の暗

号化データを前記一時記憶手段から消去するファイル管理手段を有する請求項1
1に記載の受信装置。

【請求項13】 第1の暗号化データの処理状態を示す状態情報を送信する前
記権利管理手段を有する請求項8乃至請求項12いずれかに記載の受信装置。

【請求項14】 前記権利情報を第1の権利情報と第2の権利情報とに分割す
る権利管理手段と、

前記多重化信号のうちの前記権利情報を第2の権利情報に書き換えて修正多重
化信号を出力する多重化修正手段と、

第2の受信装置からの要求信号に応じて前記修正多重化信号を第2の受信装置
に出力する請求項8乃至請求項13に記載の受信装置。

【請求項15】 前記権利情報を第1の権利情報と第2の権利情報とに分割す
る権利管理手段と、

第2の受信装置からの要求信号に応じて第2の権利情報と前記多重化信号を第
2の受信装置に出力する請求項8乃至請求項13いずれかに記載の受信装置。

【請求項16】 前記権利管理手段は第2の受信装置における第1の暗号化デ
ータの処理状態を示すデータを受信し自身と第2の受信装置の処理状態を示す状
態情報を送信することを特徴とする請求項8乃至請求項15いずれかに記載の受
信装置。

【請求項17】 第1の暗号化データを第2の暗号化データに変換する変換手
段と、

第2の暗号化データを第2の権利情報とともに再多重化する再多重化手段を有
する請求項8乃至請求項16いずれかに記載の受信装置。

【請求項18】 第1の権利情報によって第1の暗号化データを処理する請求
項8乃至請求項17いずれかに記載の受信装置。

【請求項19】 第1の暗号化データを第2の受信手段に転送後、前記第1の
暗号化データを前記一次記憶手段から消去するファイル管理手段を有する請求項
14乃至請求項18いずれかに記載の受信装置。

【請求項20】 前記多重化信号からビデオデータを抽出し復号するビデオ復
号手段を有する請求項8乃至請求項19いずれかに記載の受信装置。

【請求項21】 前記多重化信号からオーディオデータを抽出し復号するオーディオ復号手段を有する請求項8乃至請求項19いずれかに記載の受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、画像圧縮された動画と番組情報を多重化したデジタル放送信号を送信する装置、及び受信する装置に関するものである。

【0002】

【従来の技術】

図15は、従来例における送信装置と受信装置を示すブロック図である。図15において、49は入力デジタルビデオ信号、50は入力デジタルオーディオ信号、56はMPEG-2ビデオ（ISO/IEC13818-2）に準拠したビデオ符号化手段、57はMPEG-2オーディオ（ISO/IEC13818-3）に準拠したオーディオ符号化手段、64はオーディオビットストリーム、76はビデオビットストリーム、59はプログラム仕様情報生成手段、500はプログラム仕様情報、66はMPEG-2システムズ（ISO/IEC-13818-1）に準拠した多重化手段、501は多重化ビットストリーム、107は多重化分離手段、110はビデオビットストリーム、126はオーディオビットストリーム、112はビデオ復号手段、113はオーディオ復号手段、111はデジタルビデオ信号、114はデジタルオーディオ信号、503は受信装置である。

【0003】

図15にて、従来の送信装置502では、入力デジタルビデオ信号49は、ビデオ符号化手段56によってMPEG-2ビデオに準拠して圧縮符号化されビデオビットストリーム76として出力される。入力デジタルオーディオ信号50は、オーディオ符号化手段57によって圧縮符号化されオーディオビットストリーム64として出力される。プログラム仕様情報生成手段59は、ビデオビットストリーム76、オーディオビットストリーム64とプログラム番号との関係を示すプログラム仕様情報500を生成する。多重化手段66はビデオビットス

トリーム76、オーディオビットストリーム64、プログラム仕様情報500を多重化して多重化ビットストリーム501を生成する。

【0004】

従来の受信装置503では、多重化情報500は多重化分離手段107によってビデオビットストリーム110、オーディオビットストリーム126とに分離される。ビデオビットストリーム110はビデオ復号手段111によって伸長されデジタルビデオ信号112として出力される。オーディオビットストリーム126はオーディオ復号手段113によって伸長されデジタルオーディオ信号114として出力される。

【0005】

【発明が解決しようとする課題】

しかしながら、上記において、ビデオビットストリーム等の暗号化は行われておらず、不正な受信装置によって容易に盗むことが可能である。また、仮に暗号化を施しても暗号化手法自体を不正に解読されることに対する対処もなされていない。すなわち、送信装置が送信したデータの不正な受信を防ぐ手段がないという課題がある。

【0006】

本発明は、上記課題を考慮し、送信装置が送信したデータを受信装置が安全に受信する保護手段を提供することを目的とするものである。

【0007】

【課題を解決するための手段】

上述した課題を解決するために、第1の発明（請求項1に対応）は、データを暗号化して第1の暗号化データを生成する暗号化手段と、第1の暗号化データと第1の暗号化データのプログラム番号との対応を示すテーブルを含むプログラム仕様情報を生成するプログラム仕様情報手段と、第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを生成するツールリスト生成手段と、前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、第1の暗号化データに付随する権利情報を生成する権利情報生成手段と、第1の暗号化データと前記プログラム仕様情報と前記ツール

リストと前記制御グラフと前記権利情報とを多重化する多重化手段とを有する送信装置である。

【0008】

また、第2の発明（請求項2に対応）は、データを暗号化して第1の暗号化データを生成する暗号化手段と、第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを生成するツールリスト生成手段と、前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、第1の暗号化データに付随する権利情報を生成する権利情報生成手段と、第1の暗号化データと第1の暗号化データのプログラム番号との対応を示すテーブルと前記ツールリストと前記制御グラフと前記権利情報とを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、第1の暗号化データと前記プログラム仕様情報を多重化する多重化手段とを有する送信装置である。

【0009】

また、第3の発明（請求項3に対応）は、データを暗号化して第1の暗号化データを生成する暗号化手段と、第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを生成するツールリスト生成手段と、前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、第1の暗号化データと第1の暗号化データのプログラム番号との対応を示すテーブルと前記ツールリストと前記制御グラフと前記権利情報とを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、前記データに付随する権利情報を生成する権利情報生成手段と、前記権利情報を出力する権利情報送信手段と、第1の暗号化データと前記プログラム仕様情報を多重化して出力する多重化手段とを有する送信装置である。

【0010】

また、第4の発明（請求項4に対応）は、前記権利情報と前記データとの対応付けを行う前記権利情報送信手段を有する第3の発明に記載の送信装置。

【0011】

また、第5の発明（請求項5に対応）は、前記権利情報と前記データとの対応付けを行う前記プログラム仕様情報生成手段を有する第3の発明に記載の送信裝

置である。

【0012】

また、第6の発明（請求項6に対応）は、暗号を復号する復号ツールを多重化する前記多重化手段を有する第1の発明乃至第5の発明いずれかに記載の送信装置。

【0013】

また、第7の発明（請求項7に対応）は、暗号を復号するための鍵情報を多重化する前記多重化手段を有する第1の発明乃至第6の発明いずれかに記載の送信装置。

【0014】

また、第8の発明（請求項8に対応）は、第1の暗号化データを含む多重化信号を少なくとも第1の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、前記多重化信号から第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを分離するツールリスト分離手段と、前記多重化信号から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、前記多重化信号から第1の暗号化データに付随する権利情報を分離する権利情報手段と、前記ツールリストから取得したツールIDに従ってツールを入手し、前記制御グラフに従って前記ツールを組み込む第1の制御手段と、前記権利情報に従って第1の暗号化データを処理する第1の権利管理手段とを有する受信装置である。

【0015】

また、第9の発明（請求項9に対応）は、第1の暗号化データを含む多重化信号を少なくとも第1の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、前記プログラム仕様情報から第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを分離するツールリスト分離手段と、前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、前記プログラム仕様情報から第1の暗号化データに付随する権利情報を分離する権利情報手段と、前記ツールリストから取得したツールIDを有するツールを前記制御グラフに従って組み込む第

1の制御手段と、前記権利情報に従って第1の暗号化データを処理する第1の権利管理手段とを有する受信装置である。

【0016】

また、第10の発明（請求項10に対応）は、第1の暗号化データを含む多重化信号を少なくとも第1の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、前記プログラム仕様情報から第1の暗号化データを復号する復号ツールを示すツールIDを有するツールリストを分離するツールリスト分離手段と、前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、前記ツールリストから取得したツールIDを有するツールを前記制御グラフに従って組み込む第1の制御手段と、第1の暗号化データに付随する権利情報を受信する権利情報受信手段と、前記権利情報に従って第1の暗号化データを処理する第1の権利管理手段とを有する受信装置である。

【0017】

また、第11の発明（請求項11に対応）は、受信した第1の暗号化データを一時的に記憶する一時記憶手段と、前記一時記憶手段に記憶された第1の暗号化データを読み取る読み取り手段を有する第8の発明乃至第10の発明いずれかに記載の受信装置である。

【0018】

また、第12の発明（請求項12に対応）は、前記権利情報に記述された再生許諾が満了した後に第1の暗号化データを前記一時記憶手段から消去するファイル管理手段を有する第11の発明に記載の受信装置である。

【0019】

また、第13の発明（請求項13に対応）は、第1の暗号化データの処理状態を示す状態情報を送信する前記権利管理手段を有する第8の発明乃至第12の発明いずれかに記載の受信装置である。

【0020】

また、第14の発明（請求項14に対応）は、前記権利情報を第1の権利情報と第2の権利情報とに分割する権利管理手段と、前記多重化信号のうちの前記権

利情報を第2の権利情報に書き換えて修正多重化信号を出力する多重化修正手段と、第2の受信装置からの要求信号に応じて前記修正多重化信号を第2の受信装置に出力する第8の発明乃至第12の発明いずれかに記載の受信装置である。

【0021】

また、第15の発明（請求項15に対応）は、前記権利情報を第1の権利情報と第2の権利情報とに分割する権利管理手段と、第2の受信装置からの要求信号に応じて第2の権利情報と前記多重化信号を第2の受信装置に出力する第8の発明乃至第13の発明いずれかに記載の受信装置である。

【0022】

また、第16の発明（請求項16に対応）は、前記権利管理手段は第2の受信装置における第1の暗号化データの処理状態を示すデータを受信し自身と第2の受信装置の処理状態を示す状態情報を送信することを特徴とする第8の発明乃至第15の発明いずれかに記載の受信装置である。

【0023】

また、第17の発明（請求項17に対応）は、第1の暗号化データを第2の暗号化データに変換する変換手段と、第2の暗号化データを第2の権利情報とともに再多重化する再多重化手段を有する第8の発明乃至第16の発明いずれかに記載の受信装置である。

【0024】

また、第18の発明（請求項18に対応）は、第1の権利情報によって第1の暗号化データを処理する第8の発明乃至第17の発明いずれかに記載の受信装置である。

【0025】

また、第19の発明（請求項19に対応）は、第1の暗号化データを第2の受信手段に転送後、前記第1の暗号化データを前記一次記憶手段から消去するファイル管理手段を有する第14の発明乃至第18の発明いずれかに記載の受信装置である。

【0026】

また、第20の発明（請求項20に対応）は、前記多重化信号からビデオデー

タを抽出し復号するビデオ復号手段を有する第8の発明乃至第19の発明いずれかに記載の受信装置である。

【0027】

また、第21の発明（請求項21に対応）は、前記多重化信号からオーディオデータを抽出し復号するオーディオ復号手段を有する第8の発明乃至第19の発明いずれかに記載の受信装置である。

【0028】

【発明の実施の形態】

以下、本発明の実施の形態について、図1～図14を用いて説明する。

【0029】

(第1の実施の形態)

図1は、本発明の第1の実施の形態における送信装置を示すブロック図である。図1において、49、50、56、57、59、64、76は図15に示す従来例の構成と同様であり、51は権利情報生成手段、52はツールリスト生成手段、53は制御グラフ生成手段、58はストリーム情報生成手段、60はAES (Advanced Encryption Standard) に準拠した鍵長128ビットの暗号化を行う暗号化手段、61はプログラム仕様情報生成手段、62はMPEG-2システムズ (ISO/IEC-13818-1) に準拠した多重化手段、63は暗号化ビデオビットストリーム、65はプログラム仕様情報、66は多重化ビットストリーム、67は権利情報生成手段51によって生成される権利情報、68はツールリスト生成手段52によって生成されるツールリスト、69は制御グラフ生成手段53によって生成される制御グラフ、72はストリーム情報、73は第1の送信装置、74は状態情報、75は送信制御手段、81は権利制御情報、82はツール制御情報、83はグラフ制御情報、115は復号ツールである。

【0030】

図1にて、入力デジタルビデオ信号49は、ビデオ符号化手段56によってMPEG-2準拠のビデオビットストリーム76に圧縮符号化され、第1の暗号化手段60によって暗号化され暗号化ビデオビットストリーム63として出力さ

れる。入力デジタルオーディオ信号 50 は、オーディオ符号化手段 57 によって圧縮符号化されオーディオビットストリーム 64 として出力される。

【0031】

表1に状態情報 74 を示す。表1に示す各値は8ビットで表され、ビット7～ビット0で表されるものとする。送信デバイスIDをもつ送信装置から受信デバイスIDをもつ受信装置との間で状態情報及び内容を交信する。状態情報は表1に示す各値をもつものとし、内容の項にその内容を記入する。

【0032】

【表1】

状態情報	
ツール要求	0X10000000
コンテンツ要求	0X01000000
コピー情報	0X00100000
再生回数	0X00010000
編集	0X00001000

【0033】

権利情報生成手段 51 は、コンテンツ毎にコンテンツの利用条件を示す権利情報を作成してプログラム仕様情報生成手段 59 に供給する。表2の値は、状態情報が各々コピー情報、再生回数、編集である場合に対応して表1の内容のところに記入される。ここでプログラムとはコンテンツにプログラム仕様情報を付加した番組を示すこととする。

【0034】

【表2】

コピー情報	1回	0X00000000
	禁止	0X00000001
再生回数		1Xnnnnnnnn
編集	許可	0X00000010
	禁止	0X00000011

【0035】

本発明の第1の実施の形態では、A、Bの2種類のプログラムを含むものとする。プログラムAは表3に示す値で送るものとする。すなわち、コピー1回、再生回数1回、編集禁止である。

【0036】

【表3】

コンテンツ		プログラムA
コピー	1回	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【0037】

プログラムBは表4に示す値で送るものとする。すなわち、コピー1回、再生回数3回、編集禁止である。

【0038】

【表4】

コンテンツ		プログラムB
コピー	1回	0X00000000
再生回数		1X00000003
編集	禁止	0X00000011

【0039】

送信装置73は、AES復号を実行するツールID(0X00A)を有する復号ツール115が存在することを認識しているものとする。ツールリスト生成手段52は、受信装置側等で必要となるツールの一覧表を生成してプログラム仕様情報生成手段59に供給する。ツールリスト生成手段52では、MPEG-2ビデオビットストリームを受信し再生するために復号ツール115が必要であることを示し上記ツールID(0X00A)を有するツールリストを生成する。

【0040】

制御グラフ69の構成の一部を図2に示す。プログラムAは暗号化ビデオビットストリーム63とオーディオビットストリーム64を含み、暗号化ビデオビットストリーム63に対応するツールID、ツールの組み込み位置を示す制御ポイントを有している。プログラムBも同様である。

【0041】

制御グラフ生成手段53は、AES復号を実行するツールID(0X00A)を有するツールの組み込み位置が受信装置のビデオ復号手段の直前であることを示す制御グラフ69を生成してプログラム仕様情報生成手段61に出力する。

【0042】

プログラム仕様情報生成手段61は、暗号化ビデオビットストリーム63とオーディオビットストリーム64とプログラムのプログラム番号との関係を示す関係表とともに権利情報67、ツールリスト68、制御グラフ69を含むプログラム仕様情報65を生成する。

【0043】

ストリーム情報生成手段58は、暗号化手段60で用いられている暗号を解く為の鍵情報などが入ったストリーム情報72を作成する。

【0044】

多重化手段62は暗号化ビデオビットストリーム63、オーディオビットストリーム64、プログラム仕様情報65、ストリーム情報72、復号ツール115をMPEG-2システムズに準拠して多重化し、多重化ビットストリーム66を生成する。

【0045】

また、送信制御手段75は状態情報74を他の機器から受け取ることによって、本発明の第1の実施の形態の送信装置が許諾した権利情報67が他の機器でどのように処理されたかを知ることができる。ここでは、表4に示すプログラムBの権利情報が表5に示す状態情報74として本発明の送信装置で受信されたとすると、1回コピーされ、2回再生されたことがわかる。

【0046】

【表5】

コンテンツ	プログラムB
コピー	禁止 0X00000001
再生回数	1X00000001
編集	禁止 0X00000011

【0047】

以上のように、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部として受信装置にダウンロードすることができるのでツールを更新することが可能であり、常に最新の保護方式を提供するとともに、多重化情報のプログラ

ム仕様情報の一部として処理することができるという利便性を送信装置を提供することができる。

【0048】

また、本発明の第1の実施の形態では、権利情報67、ツールリスト68、制御グラフ69をプログラム仕様情報生成手段59に加えているがプログラム仕様情報生成手段59を経ずに直接多重化情報生成手段62に加えてもよい。この場合には、権利情報67、ツールリスト68、制御グラフ69はプログラム仕様情報に含まれないのでより簡便な送信装置を提供することができる。

【0049】

(第2の実施の形態)

図3は、本発明の第2の実施の形態における送信装置を示すブロック図である。図3において、49、50、56、57、64、76は図15に示す従来例の構成と同様であり、51～53、58、60～63、65～69、72、74、75、81～83は図1に示す本発明の第1の実施の形態と同様であり、84は権利情報送信手段、85は送信権利情報、86は第2の送信装置である。

【0050】

図3にて、入力ディジタルビデオ信号49は、ビデオ符号化手段56によってMPEG-2準拠のビデオビットストリーム76に圧縮符号化され、暗号化手段60によって暗号化され暗号化ビデオビットストリーム63として出力される。入力ディジタルオーディオ信号50は、オーディオ符号化手段57によって圧縮符号化されオーディオビットストリーム64として出力される。

【0051】

状態情報74は表1と同様であり、権利情報生成手段51は、コンテンツ毎にコンテンツの利用条件を示す権利情報67を作成して権利情報送信手段84に供給する。表6に権利情報67を示す。

【0052】

【表6】

コピー	1回	0X00000000
禁止		0X00000001
再生回数		1Xnnnnnnnn
編集	許可	0X00000010
	禁止	0X00000011

【0053】

本発明の第2の実施の形態では、プログラムA、プログラムBの2種類のコンテンツを含むものとする。プログラムAは表7に示す値で送るものとする。すなわち、コピー1回、再生回数1回、編集禁止である。表7で権利情報はプログラムAとの対応付けが行われている。

【0054】

【表7】

コンテンツ		プログラムA
コピー	1回	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【0055】

プログラムBは表8に示す値で送るものとする。すなわち、コピー1回、再生回数3回、編集禁止である。表8で権利情報はプログラムBとの対応付けが行われている。

【0056】

【表8】

コンテンツ		プログラムB
コピー	1回	0X00000000
再生回数		1X00000003
編集	禁止	0X00000011

【0057】

送信装置86は、AES復号を実行するツールID(0X00A)を有する復号ツール115があることを認識しているものとする。ツールリスト生成手段52は、受信装置側等で必要となるツールの一覧表を生成してプログラム仕様情報生成手段61に供給する。すなわち、MPEG-2ビデオビットストリームを受

信し再生するために復号ツール115が必要であることを示し上記ツールID（0X00A）を有するツールリスト68を生成する。

【0058】

制御グラフの構成は図2と同様である。プログラムAは第1の暗号化ビットストリーム63とオーディオビットストリーム64を含み、第1の暗号化ビットストリーム63に対応するツールID、ツールが組み込まれる組み込み位置を示す制御ポイントを有している。プログラムBも同様である。

【0059】

制御グラフ生成手段53は、上記AES復号を実行するツールID（0X00A）を有するツールの組み込み位置が受信装置のビデオ復号手段の手前であることを示す制御グラフ69を生成してプログラム仕様情報生成手段61に出力する。

【0060】

プログラム仕様情報生成手段61は、暗号化ビデオビットストリーム63とオーディオビットストリーム64とプログラムのプログラム番号との関係を示す関係表とともにツールリスト68、制御グラフ69と復号ツール115を含むプログラム仕様情報65を生成する。

【0061】

ストリーム情報生成手段58は、暗号化手段60で用いられている暗号を解く為の鍵情報などが入ったストリーム情報72を作成する。

【0062】

多重化手段62は暗号化ビデオビットストリーム63、オーディオビットストリーム64、プログラム仕様情報65、ストリーム情報72を上記MPEG-2システムズに準拠して多重化し、多重化ビットストリーム66を生成する。

【0063】

権利情報送信手段84は、権利情報67とプログラムとの対応付けを行う。ここでは、プログラム仕様情報生成手段との通信によって暗号化ビデオビットストリーム63とオーディオビットストリーム64とプログラムのプログラム番号との関係を示す関係表が得られるのでプログラムとの対応付けを行うことができ、

その後、ファイル化して送信権利情報85として送信する。権利情報を上記多重化情報とは別のファイルで送るので、権利情報を多重化情報とは別に扱うことができるので受信装置で権利情報を書き換えて別の受信装置に転送する場合に再多重化を行う必要がないという利点がある。

【0064】

また、送信制御手段75は状態情報74を他の機器から受け取ることによって、本発明の第1の実施の形態の送信装置が許諾した権利情報67が他の機器でどのように処理されたかを知ることができる。ここでは、表8に示す権利情報が表9に示す権利情報として本発明の送信装置で受信されたとすると、1回コピーされ、2回再生されたことがわかる。

【0065】

【表9】

コピー	禁止	0X00000001
再生回数		1X00000001
編集	禁止	0X00000011

【0066】

以上のように、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部として受信装置にダウンロードすることができるのでツールを更新することができたり、常に最新の保護方式を提供するとともに、権利情報を上記多重化情報とは別のファイルで送るので、権利情報を多重化情報とは別に扱うことができるので受信装置で権利情報を書き換えて別の受信装置に転送する場合に再多重化を行う必要がないという利便性を送信装置を提供することができる。

【0067】

また、本発明は、上記効果に加えて、権利情報を上記多重化情報とは別のファイルで送るとともに権利情報と多重化情報との対応付けも行うことができるので、複数の多重化情報と権利情報が混在する場合にも各々区別することができるという利便性を有する送信装置を提供することができる。

【0068】

(第3の実施の形態)

図4は、本発明の第3の実施の形態における受信装置を示すブロック図である。図4において、111～114は図15に示す従来例の構成と同様であり、100は第1の受信装置、101は入力されるMPEG-2システムズ準拠の第1の多重化ビットストリーム、102はハードディスク記憶手段、103はハードディスク記憶手段102から読み出された読み出し多重化ビットストリーム、108は組み込み手段、110はビデオビットストリーム、115はAES暗号を復号する復号ツール、120は第1の制御手段、121は第1の権利管理手段、123はファイル管理情報、124はファイル管理手段、125はハードディスク102に対する指令、90はストリーム情報及び復号ツール115を含む読み出し情報、91はプログラム仕様情報分離手段、92はプログラム仕様情報、93は制御グラフ分離手段、94は制御グラフ情報、95はツールリスト分離手段、96はツールリスト、97は権利情報分離手段、98は権利情報、132は第1の返信情報、137は第1の要求情報である。また、第1の受信装置100は第1の送信装置73に接続されているものとする。

【0069】

図4にて、入力されるMPEG-2システムズ準拠の第1の多重化ビットストリーム101はハードディスク102に一時的に記憶された後に読み出され読み出し多重化ビットストリーム103として多重化分離手段104に加えられる。多重化分離手段104は読み出し多重化ビットストリーム103を第1の暗号化ビデオビットストリーム105とオーディオビットストリーム106とプログラム仕様情報92とストリーム情報90とに分離する。

【0070】

ここで、プログラム仕様情報92は、第1の暗号化ビデオビットストリーム105、オーディオビットストリーム64とプログラムのプログラム番号との関係を示す情報とともに、上記プログラムに付随する権利情報98とAES復号を実行するツールID(0X00A)を有するツールリスト96と上記復号ツールの組み込み位置が受信装置100の多重化分離手段104とビデオ復号手段112との間であることを示す制御グラフ94を含むものとする。また、読み出し情報

90には、第1の暗号化ビデオビットストリーム105の暗号を解く為の鍵情報などが入っているものとする。

【0071】

読み出し情報90は多重化分離手段104で分離されて第1の制御手段120に加えられる。プログラム仕様情報92はプログラム仕様情報分離手段91に加えられる。制御グラフ分離手段93はプログラム仕様情報分離手段91から制御グラフ94を抽出して第1の制御手段120に供給する。ツールリスト分離手段95はプログラム仕様情報分離手段91からツールリスト96を抽出して第1の制御手段120に供給する。権利情報分離手段97はプログラム仕様情報分離手段91から権利情報98を抽出して第1の権利管理手段121に供給する。

【0072】

第1の制御手段120は表10に示す第1の要求情報137を送信する。ここではツール要求とコンテンツすなわちプログラム要求を送っている。

【0073】

【表10】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【0074】

第1の制御手段120は、ツールリスト96から復号に必要なツールが復号ツール115であることを求め、制御グラフ94から復号ツール115を適用する制御ポイントすなわち組み込み位置が108であることを求めるとともに読み出し情報90からスクランブルを解くための鍵情報を抽出する。

【0075】

第1の制御手段120は、復号ツール115の組み込み位置が受信装置100の多重化分離手段104とビデオ復号手段112との間であることを示す制御グラフ94に従って、組み込み手段108に復号ツール115とストリーム情報118から抽出された上記鍵情報が組み込む指示を出し、組み込み手段108は復号ツール115と上記鍵情報を組み込む。第1の暗号化ビデオビットストリーム105は組み込み手段108によって暗号を解読されてビデオビットストリーム

110として出力される。

【0076】

ビデオビットストリーム110はビデオ復号手段111によって伸長されディジタルビデオ信号112として出力される。オーディオビットストリーム106はオーディオ復号手段113によって伸長されディジタルオーディオ信号114として出力される。

【0077】

第1の権利管理手段121は権利情報98を取得し、ファイル管理情報123をファイル管理手段124に出力する。ファイル管理手段124は、プログラムAの場合、表4に与えられた再生回数は1回であるため、1回再生するとファイル管理手段124は、指令125をハードディスク102に出してハードディスク102上に記憶されたプログラムAを消去する。

【0078】

また、第1の権利管理手段121は第2の返信情報132として表11に示す情報を返信する。ここでは第1の受信装置100で1回再生されている。

【0079】

【表11】

コピー	許可	0X00000000
第1の受信装置での再生回数		0X00000001

【0080】

(第4の実施の形態)

図5は、本発明の第4の実施の形態における受信装置を示すブロック図である。本発明の第4の実施の形態は受信装置がネットワークを通じて接続されている別の受信装置にツールをダウンロード、ディジタルデータを転送、サーバに消費情報を転送することができる。図5において、111～114は図15に示す従来例の構成と同様であり、90～98、101～106、108、110、115、123～125、132は本発明の第3の実施の形態と同様であり、130は第2の受信装置、133は第2の権利情報、136は第2の返信情報、138は第2の権利管理手段、139は第2の制御手段、140は第2の要求情報、1

4 1 は第 1 の制御情報、 1 4 2 は多重化修正手段、 1 4 3 はM P E G - 2 システムズ準拠の第 2 の多重化ビットストリーム、 1 4 4 は第 1 0 の受信装置である。図 6 は、第 2 の権利管理手段 1 3 8 の処理の概略を示す図である。図 7 は、第 1 の多重化ビットストリーム 1 0 3 と第 2 の多重化ビットストリーム 1 4 3 の概略の構成を示す図であり、 1 4 6 は暗号化ビデオビットストリーム 6 3 とオーディオビットストリーム 6 4 とプログラム A のプログラム番号との関係を示す関係表である。また、図 5 において、第 2 の受信装置 1 3 0 は送信装置 7 3 に接続されているものとし、第 2 の受信装置 1 3 0 に接続されている第 1 0 の受信装置 1 4 4 は図 4 に示す第 1 の受信装置と等価な機能を有するものとする。

【0081】

図 5 にて、読み出し情報 9 0 は多重化分離手段 1 0 4 で分離されて第 2 の制御手段 1 3 9 に加えられる。第 2 の制御手段 1 3 9 は、第 2 の権利管理手段 1 3 8 に権利許諾の情報を出すとともに多重化修正手段 1 4 2 に多重化ビットストリーム修正を含む第 1 の制御情報 1 4 1 を送る。

【0082】

第 2 の制御手段 1 3 9 は第 1 0 の受信装置 1 4 4 から表 1 2 に示す第 2 の要求情報 1 4 0 を受け取る。表 1 2 は第 1 0 の受信装置 1 4 4 が第 2 の受信装置 1 3 0 に対してツールとコンテンツを要求していることを示している。

【0083】

【表 1 2】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【0084】

図 6 は第 2 の権利管理手段 1 3 8 の動作の一部を示している。ステップ 1 において、第 2 の制御手段 1 3 9 を経由して第 2 の要求情報 1 4 0 を受信する、ステップ 2 で権利情報 9 8 を受信し、ステップ 3 で権利情報 9 8 を第 2 の受信装置 1 3 0 で使用する第 1 の権利情報と第 1 0 の受信装置 1 4 4 で使用する第 2 の権利情報 1 3 3 に分割する。ステップ 4 で第 1 の権利情報を出力し、ステップ 5 で第 1 の権利情報に基づいてファイル管理情報 1 2 3 をファイル管理手段 1 2 4 に出

力し、ステップ6で第2の権利情報133を出力する。

【0085】

第2の受信装置130で表4に示す権利情報を有するプログラムBを1回再生するとともに第1の受信装置に転送するものとすると、第1の権利情報を表13、第2の権利情報を表14のように表わすことができる。第10の受信装置144に転送する第2の権利情報を示す表14では第2の受信装置130で1回再生するので再生回数を1回減じている。

【0086】

【表13】

コピー	禁止	0X00000001
再生回数		1X00000001
編集	禁止	0X00000011

【0087】

【表14】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【0088】

第2の権利管理手段138は表14に示す第2の権利情報133を多重化修正手段142に送る。多重化修正手段142は第1の多重化ビットストリーム103に第2の権利情報133をもとに修正を加える。すなわち、第1の多重化ビットストリーム103の権利情報122を第2の権利情報133の内容に変更して第2の多重化ビットストリーム143を出力する。

【0089】

図7は第1の多重化ビットストリームと第2の多重化ビットストリームの構成を示している。権利情報98は第2の権利管理手段によって第2の権利情報133として多重化修正手段142に加えられ、第2の多重化ビットストリーム143では第2の権利情報が含まれる。

【0090】

第2の制御手段139は、復号ツール115の組み込み位置が第2の受信装置130の多重化分離手段104とビデオ復号手段112との間であることを示す制御グラフ94に従って、組み込み手段108に復号ツール115とストリーム情報118から抽出された上記鍵情報を組み込む指示を出し、組み込み手段108は復号ツール115と上記鍵情報を組み込む。第1の暗号化ビデオビットストリーム105は組み込み手段108によって暗号を解読されてビデオビットストリーム110として出力され、ビデオ復号手段112によって復号されてデジタルビデオ信号として出力される。

【0091】

その他の動作は本発明の第3の実施の形態と同様である。これによって、第2の受信装置130は、受信した権利情報、ビットストリーム、ツール情報等をネットワーク上で接続された第10の受信装置144に送ることが可能となる。

【0092】

また、第2の権利管理手段138は、第10の受信装置144から送られる第2の返信情報136をもとにして第1の返信情報132を出力する。この場合、第2の受信装置130及び第10の受信装置144での再生回数は1回であるとすると、表15のように構成される第1の返信情報を出力する。

【0093】

【表15】

第2の受信装置での再生回数	0X00000001
第1の受信装置での再生回数	0X00000001

【0094】

これによって送信装置は、第2の受信装置130及び第2の受信装置130に接続された第10の受信装置144での消費情報を得ることができる。

【0095】

(第5の実施の形態)

図8は、本発明の第5の実施の形態における受信装置を示すブロック図である。本発明の第5の実施の形態は受信装置が受信した権利情報をダウンロード、デジタルデータをネットワークに接続されている別の受信装置に転送するととも

にサーバに消費情報を転送することができる。図8において、111～114は図15に示す従来例の構成と同様であり、90～98、101～106、108、110、115、123～125、132、137は図4に示す本発明の第3の実施の形態と同様であり、136、140は図5に示す本発明の第4の実施の形態と同様であり、150は第3の受信装置、153は第3の権利情報、154は第4の受信装置、160は第3の制御手段、161は第3の権利管理手段である。

【0096】

図8にて、第3の制御手段160は第4の受信装置154から表16に示す第2の要求情報140を受け取るものとする。表16は第4の受信装置154が第3の受信装置150に対してツールとコンテンツを要求していることを示している。第3の制御手段160は第3の権利管理手段161に権利許諾の情報を出す。

【0097】

【表16】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【0098】

読み出し情報90は多重化分離手段104で分離されて第3の制御手段160に加えられる。第3の権利管理手段161は、権利情報98を第3の受信装置150で使用する第1の権利情報と第4の受信装置154で使用する第3の権利情報153とに分割し、第3の権利情報153を第4の受信装置154に送る。

【0099】

ここでは第3の受信装置150で1回再生し、第4の受信装置154で1回再生するものとすると、第1の権利情報及び第3の権利情報153は各々表17、表18となる。表18では第3の受信装置150で1回再生しているので再生回数を1回減じている。

【0100】

【表17】

コピー	禁止	0X00000000
再生回数		1X00000001
編集	禁止	0X000000011

【0101】

【表18】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X000000011

【0102】

その他の動作は本発明の第3の実施の形態と同様である。これによって、第3の受信装置150は、受信した権利情報、ビットストリーム、ツール情報等を第4の受信装置154に送ることが可能となる。

【0103】

(第6の実施の形態)

図9は、本発明の第6の実施の形態における受信装置を示すブロック図である。本発明の第6の実施の形態は第3の受信装置にホームネットワークを経由して接続された第4の受信装置に関するものである。図9において、111～114は図15に示す従来例の構成と同様であり、90～98、101～106、108、110、115、123～125、137は図4に示す本発明の第3の実施の形態と同様であり、136は図5に示す本発明の第4の実施の形態と同様であり、154は第4の受信装置、231は第4の制御手段、232は第4の権利管理手段である。

【0104】

図9にて、読み出し情報90は多重化分離手段104で分離されて第4の制御手段231に加えられる。第4の権利管理手段232は権利情報98をもとにして、第4の受信装置154での消費状況とをもとに第2の返信情報136を生成する。第2の返信情報136は、デジタルビデオ情報112及びデジタルオーディオ情報114を第4の受信装置で再生したことと示す消費情報として再生

回数を1回減じる。その結果、表18のように与えられるプログラムBの権利情報は表19のように書き換えられる。

【0105】

【表19】

コンテンツ	許可	プログラムB
コピー	禁止	0X00000001
再生回数		1X00000001
複数	禁止	0X00000011

【0106】

表19のように書き換えられた第2の返信情報136は第4の権利管理手段232から送出される。その他の動作は図4に示す本発明の第3の実施の形態と同様である。

【0107】

(第7の実施の形態)

図10は、本発明の第7の実施の形態における受信装置を示すブロック図である。本発明の第7の実施の形態は受信装置に受信した権利情報をダウンロード、ディジタルデータを別の受信装置にデータを変換して転送するとともにサーバに消費情報を転送することができる。図10において、111～114は図15に示す従来例の構成と同様であり、90～98、101～106、110、115、123～125、132は、図4に示す本発明の第3の実施の形態と同様であり、141は図5に示す本発明の第4の実施の形態と同様であり、144は第4の権利情報、250は第5の受信装置、251は第5の権利管理手段、252は第5の制御手段、253は変換手段、254は第2の暗号化ビデオビットストリーム、255は再多重化手段、256はMPEG-2システムズ準拠の第3の多重化ビットストリーム、257は第6の受信装置、258は第3の要求情報である。

【0108】

図10にて、読み出し情報90は多重化分離手段104で分離されて第5の制御手段252に加えられる。第5の権利管理手段251は、権利情報98を第5の受信装置250で使用する第1の権利情報と第6の受信装置257で使用する

第4の権利情報144に分割し、第4の権利情報144を再多重化手段255に送る。

【0109】

第5の制御手段252は第6の受信装置257から表20に示す第3の要求情報258を受け取るものとする。表20は第6の受信装置257が第5の受信装置250に対してツールとコンテンツを要求していることを示している。第5の制御手段252は第5の権利管理手段251に権利許諾の情報を出すとともに再多重化手段255に再多重化の指示を含む第1の制御情報141を送る。

【0110】

【表20】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【0111】

ここで、第5の受信装置250で1回再生し、第6の受信装置257で1回再生するものとすると、第1の権利情報及び第4の権利情報144は各々表21、表22となる。表22では第5の受信装置250で1回再生しているので再生回数を1回減じている。

【0112】

【表21】

コピー	禁止	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【0113】

【表22】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【0114】

変換手段253はデジタルビデオデータ111をMPEG-4ビデオ（IS

O／IEC14496)に圧縮変換し更に暗号化して第2の暗号化ビデオビットストリーム254を出力する。

【0115】

復号ツール115は再多重化手段255に送られる。再多重化手段255は第2の暗号化ビデオビットストリーム254とオーディオビットストリーム126と第1の制御情報141と第4の権利情報144と復号ツール115とをMPEG-2システムズに準拠して再多重し、再多重化信号256を出力する。本発明の第7の実施の形態ではデジタルオーディオビットストリーム106を用いているがデジタルオーディオ信号114を再度圧縮して用いてもよい。

【0116】

その他の動作は図4に示す本発明の第3の実施の形態と同様である。これによって、第5の受信装置250は、受信した権利情報、ビットストリーム、ツール情報等を第6の受信装置257に送ることが可能となる。

【0117】

(第8の実施の形態)

図11は、本発明の第8の実施の形態における受信装置を示すブロック図である。図11において、111～114は図15に示す従来例の構成と同様である、90～96、98、101～106、110、115、120、121、123～125、132は、図4に示す本発明の第3の実施の形態と同様であり、300は受信権利情報、301は権利情報受信手段、302は第7の受信装置である。また、第7の受信装置は本発明の第2の実施の形態の図3に示す送信装置86に接続されているものとする。本発明の第8の実施の形態は本発明の第3の実施の形態と類似であるが、権利情報98をプログラム仕様情報92でなく受信権利情報300から取得する点が異なる。

【0118】

図11にて、入力されるMPEG-2システムズ準拠の第1の多重化ビットストリーム101はハードディスク102に一時的に記憶された後に読み出され読み出し多重化ビットストリーム103として多重化分離手段104に加えられる。多重化分離手段104は読み出し多重化ビットストリーム103を第1の暗号

化ビデオビットストリーム105とオーディオビットストリーム106とプログラム仕様情報92とストリーム情報90とに分離する。

【0119】

ここで、プログラム仕様情報92は、第1の暗号化ビデオビットストリーム105、オーディオビットストリーム64とプログラムのプログラム番号との関係を示す情報とともに、上記プログラムに付随する権利情報98とAES復号を実行するツールID(0X00A)を有するツールリスト96と上記復号ツールの組み込み位置が受信装置100の多重化分離手段104とビデオ復号手段112との間であることを示す制御グラフ94を含むものとする。また、読み出し情報90には、第1の暗号化ビデオビットストリーム105の暗号を解く為の鍵情報などが入っているものとする。

【0120】

読み出し情報90は多重化分離手段104で分離されて第1の制御手段120に加えられる。プログラム仕様情報92はプログラム仕様情報分離手段91に加えられる。制御グラフ分離手段93はプログラム仕様情報分離手段91から制御グラフ94を抽出して第1の制御手段120に供給する。ツールリスト分離手段95はプログラム仕様情報分離手段91からツールリスト96を抽出して第1の制御手段120に供給する。権利情報受信手段301は受信権利情報300を受信して権利情報98を抽出して出力し第1の権利管理手段121に供給する。

【0121】

第1の制御手段120は表23に示す第1の要求情報137を送信する。ここではツール要求とコンテンツすなわちプログラム要求を送っている。

【0122】

【表23】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【0123】

第1の制御手段120は、ツールリスト96から復号に必要なツールが復号ツール115であることを求め、制御グラフ94から復号ツール115を適用する

制御ポイントすなわち組み込み位置が108であることを求めるとともに読み出し情報90から暗号を解くための鍵情報を抽出する。

【0124】

第1の制御手段120は、復号ツール115の組み込み位置が第7の受信装置302の多重化分離手段104とビデオ復号手段112との間であることを示す制御グラフ94に従って、組み込み手段108に復号ツール115とストリーム情報118から抽出された上記鍵情報を組み込む指示を出し、組み込み手段108は復号ツール115と上記鍵情報を組み込む。第1の暗号化ビデオビットストリーム105は組み込み手段108によって暗号を解読されてビットストリーム110として出力される。

【0125】

ビデオビットストリーム110はビデオ復号手段112によって伸長されデジタルビデオ信号111として出力される。オーディオビットストリーム106はオーディオ復号手段113によって伸長されデジタルオーディオ信号114として出力される。

【0126】

第1の権利管理手段121は権利情報98を取得し、ファイル管理情報123をファイル管理手段124に出力する。ファイル管理手段124は、プログラムAの場合、表4に与えられた再生回数は1回であるため、1回再生するとファイル管理手段124は、指令125をハードディスク102に出してハードディスク102上に記憶されたプログラムAを消去する。

【0127】

また、第1の権利管理手段121は第1の返信情報132として表24に示す情報を返信する。

【0128】

【表24】

第7の受信装置での再生回数	0X00000001
---------------	------------

【0129】

(第9の実施の形態)

図12は、本発明の第9の実施の形態における受信装置を示すブロック図である。本発明の第9の実施の形態はネットワークに接続されている受信装置に受信した権利情報をダウンロード、ディジタルデータを転送するとともにサーバに消費情報を転送することができる。図12において、111～114は図15に示す従来例の構成と同様であり、90～96、98、101～106、110、115、123～125、132は本発明の第3の実施の形態と同様であり、133、136、138～140、141～143は図5に示す本発明の第4の実施の形態と同様であり、300、301は図11に示す本発明の第8の実施の形態と同様であり、310は第8の受信装置、145は第11の受信装置である。尚、第8の受信装置310は図3に示す本発明の第2の送信装置に接続されているものとし、第11の受信装置は、図4に示す第1の受信装置と同等の機能を有するものとする。

【0130】

図12にて、制御グラフ分離手段93はプログラム仕様情報分離手段91から制御グラフ94を抽出して第2の制御手段139に供給する。ツールリスト分離手段95はプログラム仕様情報分離手段91からツールリスト96を抽出して第2の制御手段139に供給する。権利情報受信手段301は受信権利情報300を受信して権利情報98を抽出して出力し第2の権利管理手段138に供給する。

【0131】

第2の制御手段139は第11の受信装置145から表25に示す第2の要求情報140を受け取るものとする。表25は第11の受信装置145が第2の受信装置130に対してツールとコンテンツを要求していることを示している。

【0132】

【表25】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【0133】

また、読み出し情報90は多重化分離手段104で分離されて第2の制御手段139に加えられる。第2の権利管理手段138は、権利情報98を第2の受信装置130で使用する第1の権利情報と第11の受信装置145で使用する第2の権利情報133に分割するとともに、第1の権利情報に基づいてファイル管理情報123をファイル管理手段124に出力する。第2の権利管理手段138に権利許諾の指示を出すとともに多重化修正手段142に第1の多重化ビットストリーム103の修正を含む第1の制御情報141を送る。

【0134】

第8の受信装置310で表4に示す権利情報を有するプログラムBを1回再生するとともに第11の受信装置145に転送するものとすると、第1の権利情報を表26、第2の権利情報133を表27のように表わすことができる。第11の受信装置145に転送する第2の権利情報を示す表27では第2の受信装置130で1回再生するので再生回数を1回減じている。

【0135】

【表26】

コピー	禁止	0X000000000
再生回数		1X000000001
編集	禁止	0X000000011

【0136】

【表27】

コピー	禁止	0X000000001
再生回数		1X000000002
編集	禁止	0X000000011

【0137】

第2の権利管理手段138は表14に示す第2の権利情報133を多重化修正手段142に送る。多重化修正手段142は第1の多重化ビットストリーム103に第2の権利情報133をもとに修正を加える。すなわち、第1の多重化ビットストリーム103の権利情報122を第2の権利情報133の内容に変更して第2の多重化ビットストリーム143を出力する。

【0138】

その他の動作は本発明の第4の実施の形態と同様である。これによって、第8の受信装置130は、受信した権利情報、ピットストリーム、ツール情報等をネットワーク上で接続された第11の受信装置145に送ることが可能となる。

【0139】

また、第2の権利管理手段138は、第11の受信装置145から送られる第2の返信情報をもとに第1の返信情報132を出力する。この場合、第8の受信装置310及び第11の受信装置145での再生回数は1回であるとすると、表28のように構成される第1の返信情報を出力する。

【0140】

【表28】

第2の受信装置での再生回数	0X00000001
第10の受信装置での再生回数	0X00000001

【0141】

これによって送信装置は、第8の受信装置310及び第8の受信装置310に接続された第11の受信装置145での消費情報を得ることができる。

【0142】

(第10の実施の形態)

図13は、本発明の第10の実施の形態における受信装置を示すブロック図である。本発明の第10の実施の形態は受信装置にホームネットワークを経由して接続された別の受信装置に関するものである。図13において、111～114は図15に示す従来例の構成と同様であり、90～96、98、101～106、110、115、123～125、132は図4に示す本発明の第3の実施の形態と同様であり、136、140は図5に示す本発明の第4の実施の形態と同様であり、153、154、160、161は図8に示す本発明の第5の実施の形態と同様であり、300、301は図11に示す本発明の第8の実施の形態と同様であり、320は第9の受信装置である。

【0143】

図13にて、制御グラフ分離手段93はプログラム仕様情報分離手段91から

制御グラフ94を抽出して第3の制御手段160に供給する。ツールリスト分離手段95はプログラム仕様情報分離手段91からツールリスト96を抽出して第3の制御手段160に供給する。権利情報受信手段301は受信権利情報300を受信して権利情報98を抽出して出力し第3の権利管理手段161に供給する。

【0144】

また、読み出し情報90は第3の制御手段160に加えられる。第3の権利情報管理手段161は、権利情報98を第9の受信装置320で使用する第1の権利情報と第4の受信装置154で使用する第3の権利情報153とに分割し、第3の権利情報153を第4の受信装置154に送る。

【0145】

第3の制御手段160は第4の受信装置154から表28に示す第2の要求情報140を受け取るものとする。表29は第4の受信装置154が第9の受信装置320に対してツールとコンテンツを要求していることを示している。第3の制御手段160は第3の権利管理手段161に権利許諾の情報を出す。

【0146】

【表29】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【0147】

ここでは第9の受信装置320で1回再生し、第4の受信装置154で1回再生するものとすると、第1の権利情報及び第3の権利情報153は各々表30、表31となる。表31では第9の受信装置320で1回再生しているので再生回数を1回減じている。

【0148】

【表30】

コピー	禁止	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【0149】

【表31】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【0150】

その他の動作は本発明の第5の実施の形態と同様である。これによって、第9の受信装置320は、受信した権利情報、ビットストリーム、ツール情報等を第4の受信装置154に送ることが可能となる。

【0151】

(第11の実施の形態)

図14は、本発明の第11の実施の形態における受信装置を示すブロック図である。本発明の第11の実施の形態は第1の送信装置73と第2の受信装置130と第2の受信装置にネットワークによって接続された第10の受信装置144に関するものである。図14において、49、50は図15に示す従来例の構成と同様であり、66、73、74は図1に示す本発明の第1の実施の形態と同様であり、111、114、130、136、140、143、144は図5に示す本発明の第4の実施の形態と同様である。

【0152】

図14にて、第10の受信装置144は第2の要求情報140を第2の受信装置130に出力する。第2の受信装置130は状態情報74を第1の送信装置73に出力する。第1の送信装置73は、本発明の第1の実施の形態と同様に第1の多重化ビットストリーム66を出力する。第2の受信装置130が受信する第1の多重化ビットストリーム66は本発明の第4の実施の形態では101と記されており、本発明の第4の実施の形態と同様に処理されてビデオ復号手段111とディジタルオーディオ信号114を出力すると共に第2の多重化ビットストリーム143として第10の受信装置144に出力される。第10の受信装置144は、本発明の第3の実施の形態と同様に動作し、第2の返信情報136を出力する。

【0153】

【発明の効果】

以上説明したところから明らかなように、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部として受信装置にダウンロードすることができるるのでツールを更新することが可能であり、常に最新の保護方式を提供することができる信頼性の高い送信装置を提供することができる。

【0154】

また、本発明は、上記効果に加えて、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報のプログラム仕様情報を一部として処理することができるという利便性を提供することができる。

【0155】

また、本発明は、上記効果に加えて、権利情報を上記多重化情報とは別のファイルで送るので、権利情報を多重化情報とは別に扱うことができるので受信装置で権利情報を書き換えて別の受信装置に転送する場合に再多重化を行う必要がないという利便性を有する送信装置を提供することができる。

【0156】

また、本発明は、上記効果に加えて、権利情報を上記多重化情報とは別のファイルで送るとともに権利情報と多重化情報との対応付けも行うことができるので、複数の多重化情報と権利情報が混在する場合にも各々区別することができるという利便性を有する送信装置を提供することができる。

【0157】

また、本発明は、上記効果に加えて、暗号を復号する復号ツールも同時に多重化して送信する利便性を有する送信装置を提供することができる。

【0158】

また、本発明は、上記効果に加えて、暗号を復号するための鍵情報も同時に多重化して送信する利便性を有する送信装置を提供することができる。

【0159】

本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部としてダウンロードすることができるので更新可能であり、常に最新の保護方式を組み込むことができる信頼性の高い受信装置を提供することができる。

【0160】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持することができるばかりでなく、多重化情報のプログラム仕様情報の一部として処理できる利便性を有する受信装置を提供することができる。

【0161】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持することができるばかりでなく、権利情報を上記多重化情報とは別のファイルで受信することができるので権利情報を多重化情報とは別に扱うことができるという利便性と別の受信装置に転送する場合の任意性を与えることができる受信装置を提供することができる。

【0162】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、権利情報に基づいて受信した暗号化データを消去することができるので使用済みのコンテンツを受信装置に残すことがなく不正な使用を防止することができる信頼性の高い受信装置を提供することができる。

【0163】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、受信した暗号化データの消費情報を送信装置に送り受信装置の消費状況を提供する受信裝

置を提供することができる。

【0164】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報を別の受信装置にダウンロードすることができるので更新可能であり、常に最新の保護方式を維持できることに加えて、別の受信装置が受信した暗号化データの消費情報を送信装置に送り受信装置の消費状況を提供する受信装置を提供することができる。

【0165】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、受信した権利情報を分割して別の受信装置に暗号化データとともに送信することができるので別の受信装置でも同様に暗号化データを高信頼性のもとに処理することのできる受信装置を提供することができる。

【0166】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、受信装置が受信したデータを変換することにより別の受信装置に最適な信号として転送することができる受信装置を提供することができる。

【図面の簡単な説明】

【図1】

本発明の第1の実施の形態における送信装置の概略構成を示す図

【図2】

本発明の第1の実施の形態における制御グラフ

【図3】

本発明の第2の実施の形態における送信装置の概略構成を示す図

【図4】

本発明の第3の実施の形態における受信装置の概略構成を示す図

【図5】

本発明の第4の実施の形態における受信装置の概略構成を示す図

【図6】

本発明の第4の実施の形態における第2の権利管理手段の概略処理を示す図

【図7】

本発明の第4の実施の形態における多重化ビットストリームの概略構成を示す

図

【図8】

本発明の第5の実施の形態における受信装置の概略構成を示す図

【図9】

本発明の第6の実施の形態における受信装置の概略構成を示す図

【図10】

本発明の第7の実施の形態における受信装置の概略構成を示す図

【図11】

本発明の第8の実施の形態における受信装置の概略構成を示す図

【図12】

本発明の第9の実施の形態における受信装置の概略構成を示す図

【図13】

本発明の第10の実施の形態における受信装置の概略構成を示す図

【図14】

本発明の第11の実施の形態におけるシステム構成を示す図

【図15】

従来の構成図

【符号の説明】

5 1 権利情報生成手段

5 3 制御グラフ生成手段

5 4 制御情報生成手段

6 0 暗号化手段

6 3 暗号化ビデオビットストリーム

- 7 3 第1の送信装置
- 7 4 状態情報
- 8 5 送信権利情報
- 9 0 読み出し情報
- 9 5 ツールリスト分離手段
- 9 7 権利情報分離手段
- 1 0 1 第1の多重化ビットストリーム
- 1 0 8 組み込み手段
- 1 1 5 復号ツール
- 1 2 0 第1の制御手段
- 1 2 1 第1の権利管理手段
- 1 2 4 ファイル管理手段
- 1 3 2 第1の返信情報
- 1 3 3 第2の権利情報
- 1 3 6 第2の返信情報
- 1 3 7 第1の要求情報
- 1 3 8 第2の権利管理手段
- 1 3 9 第2の制御手段
- 1 4 0 第2の要求情報
- 1 4 1 第1の制御情報
- 1 4 3 第2の多重化ビットストリーム
- 1 5 3 第3の権利情報
- 1 6 0 第3の制御手段
- 1 6 1 第3の権利管理手段
- 2 3 1 第4の制御手段
- 2 3 2 第4の権利管理手段
- 2 5 1 第5の権利管理手段
- 2 5 2 第5の制御手段
- 2 5 4 第2の暗号化ビデオビットストリーム

255 再多重化手段

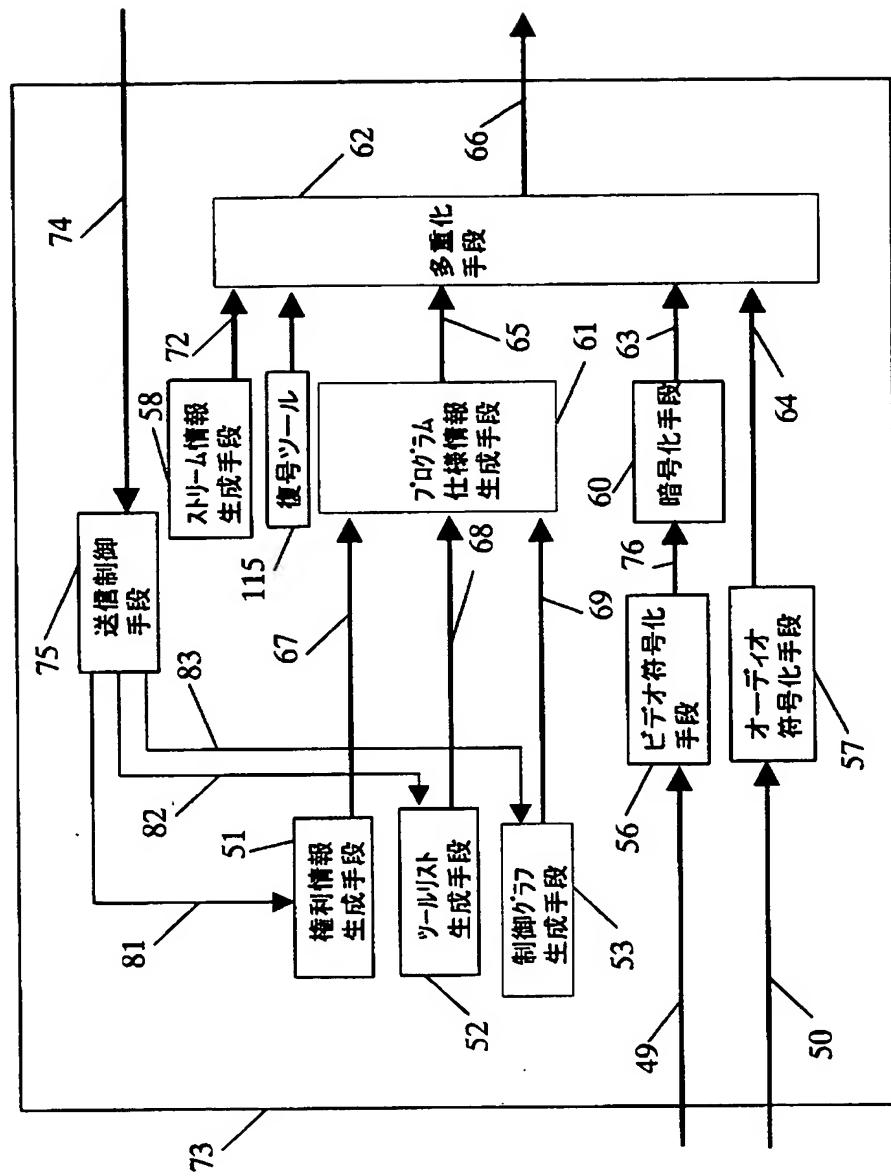
256 第3の多重化ビットストリーム

258 第3の要求情報

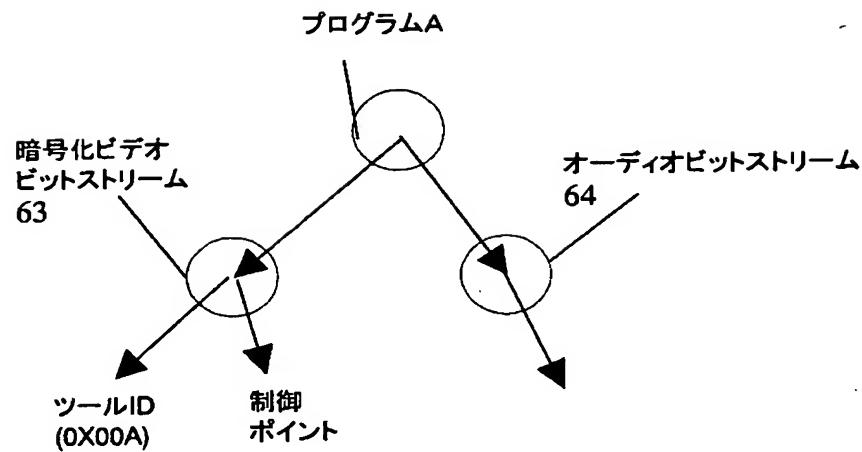
【書類名】

図面

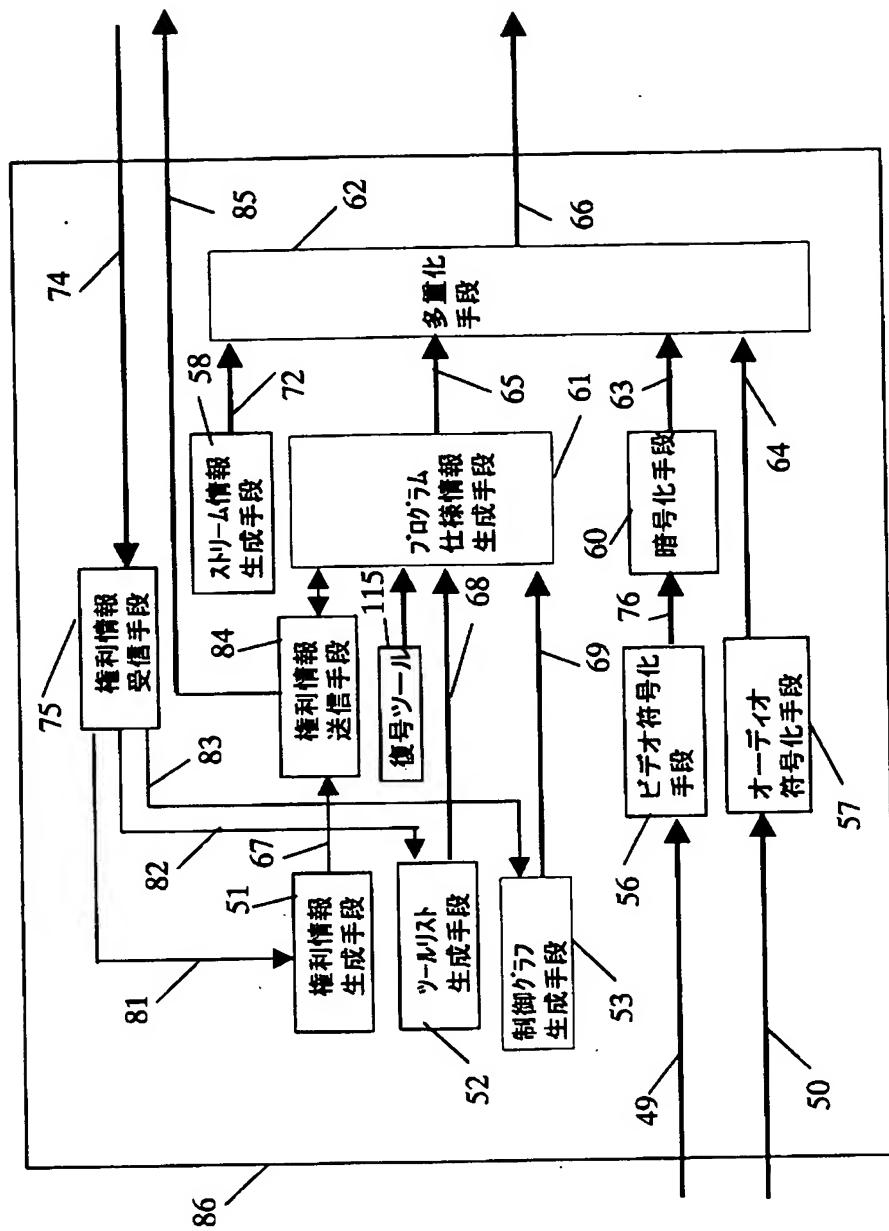
【図1】



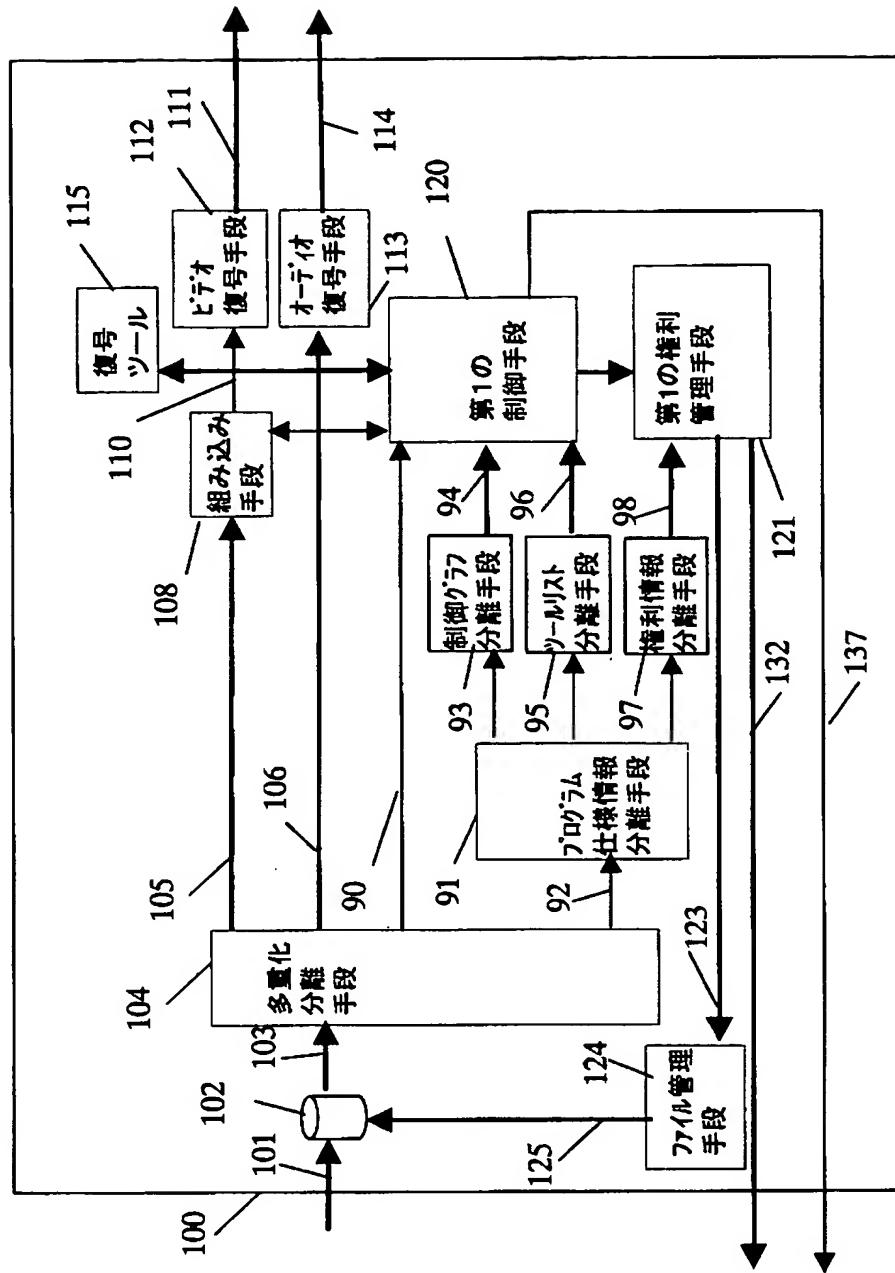
【図2】



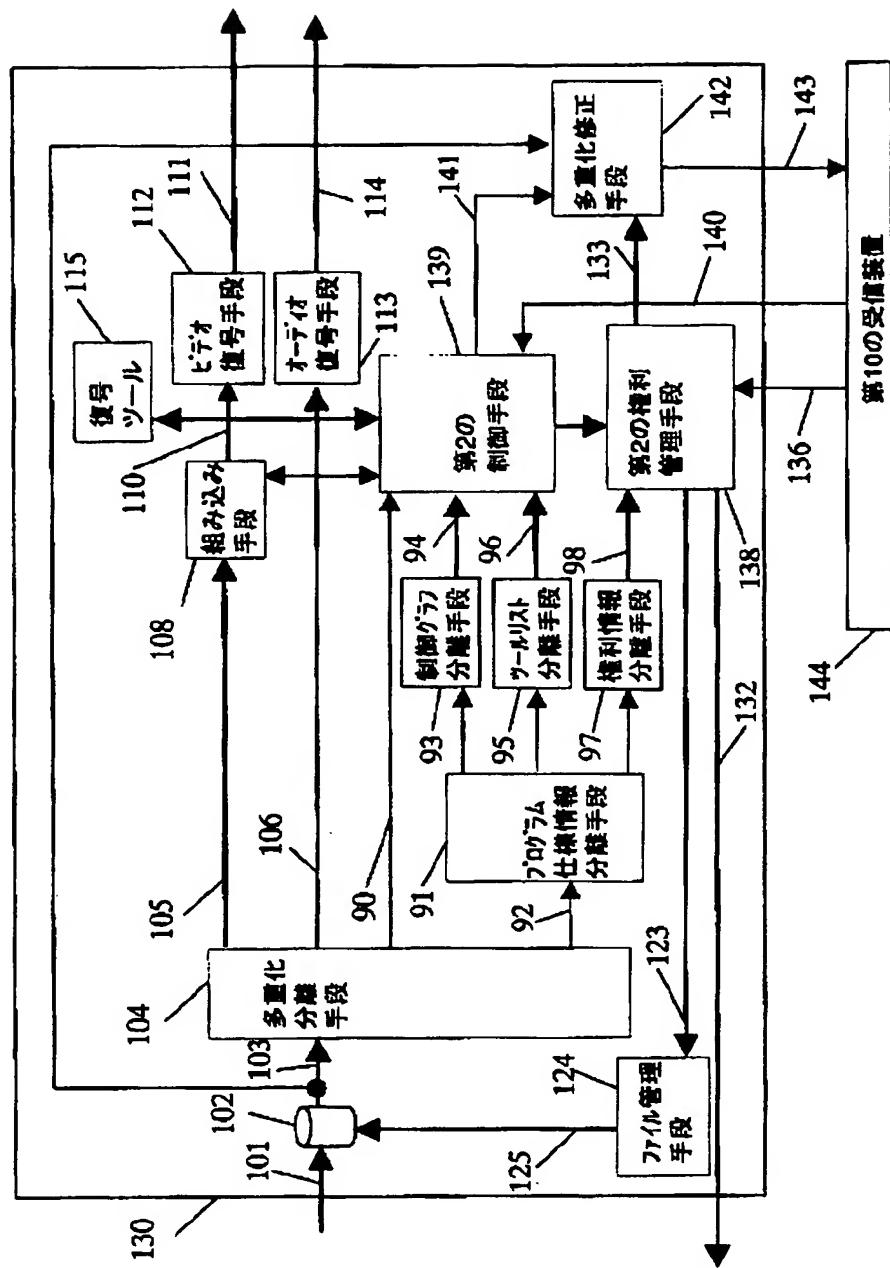
【図3】



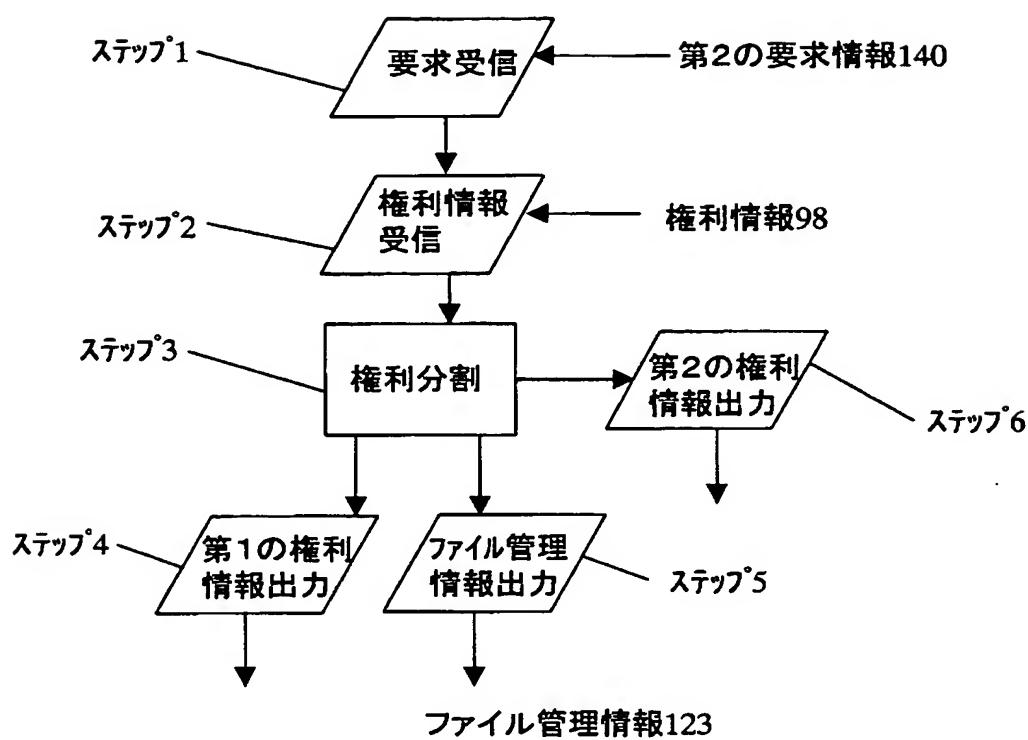
【図4】



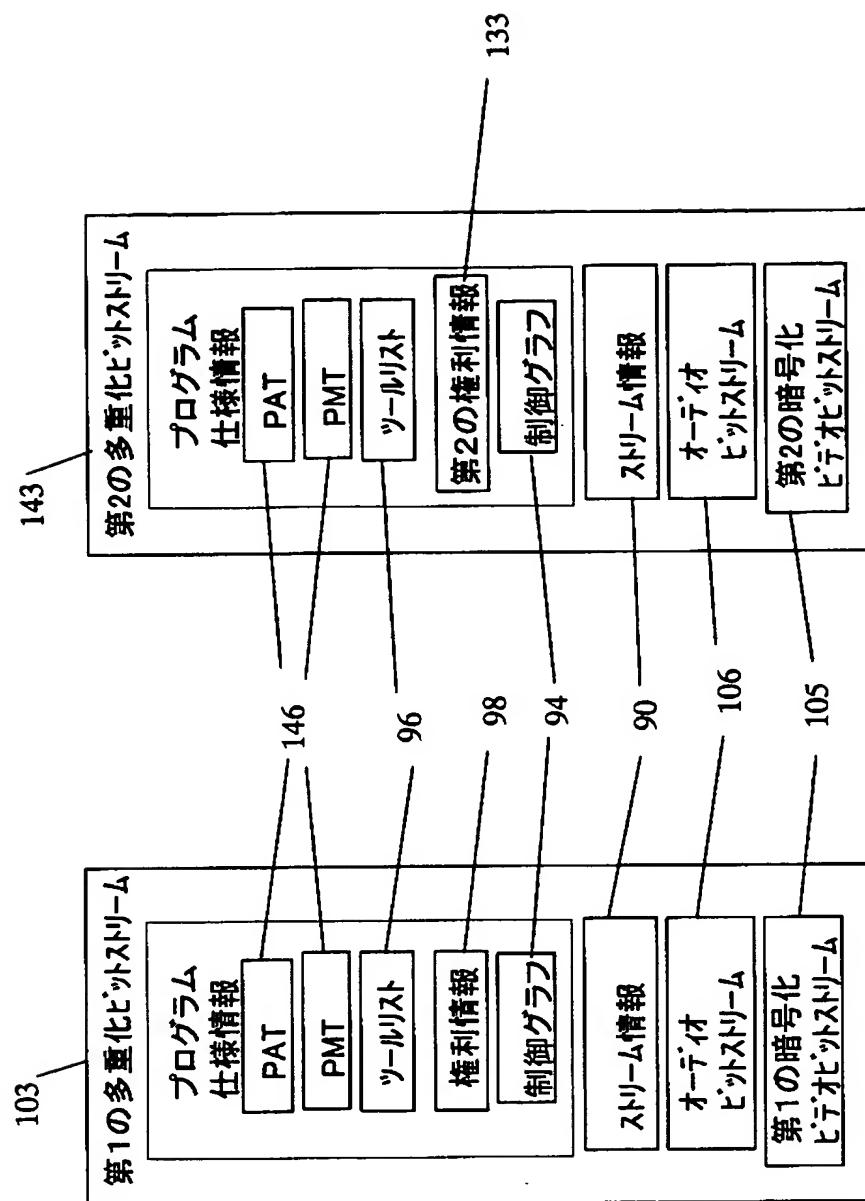
【図5】



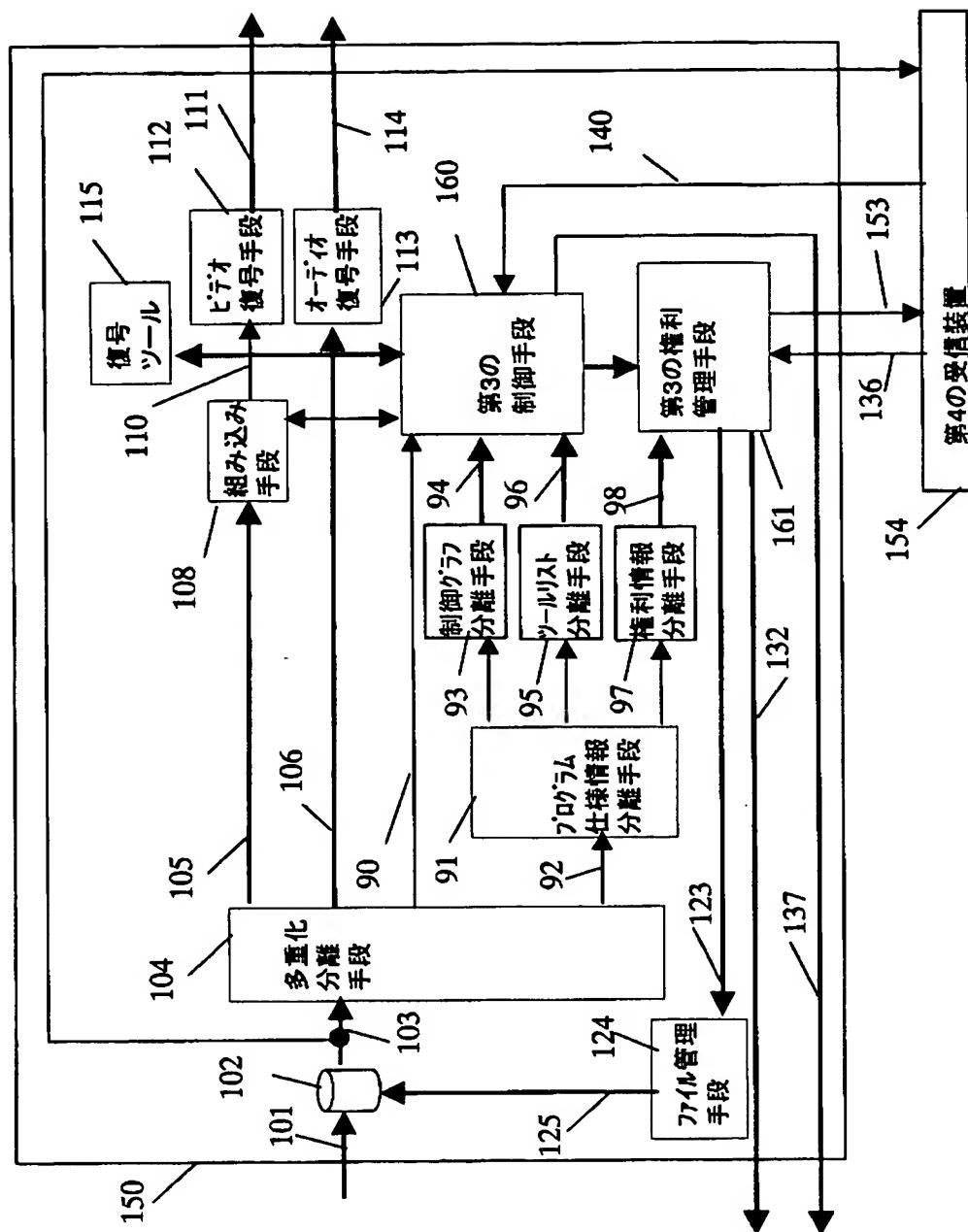
【図6】



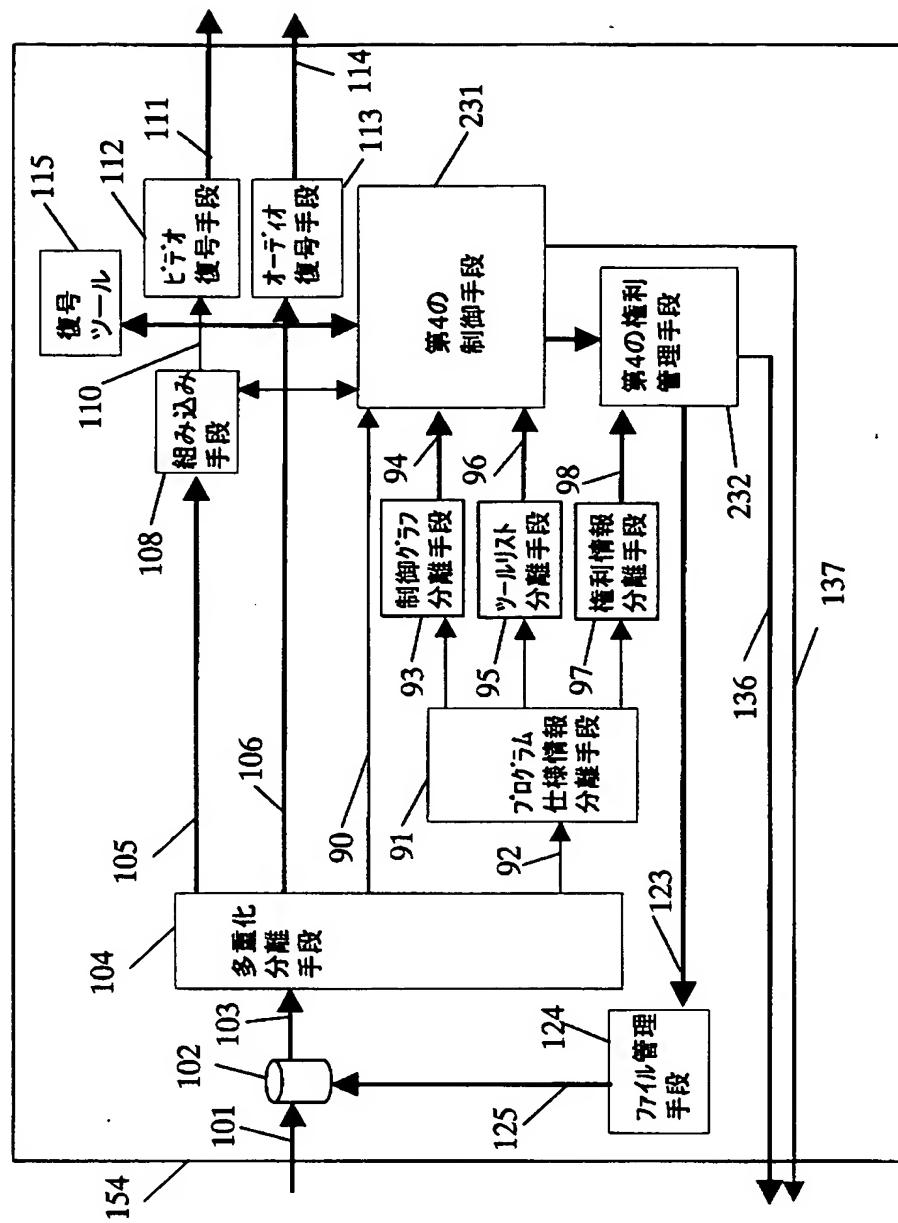
【図7】



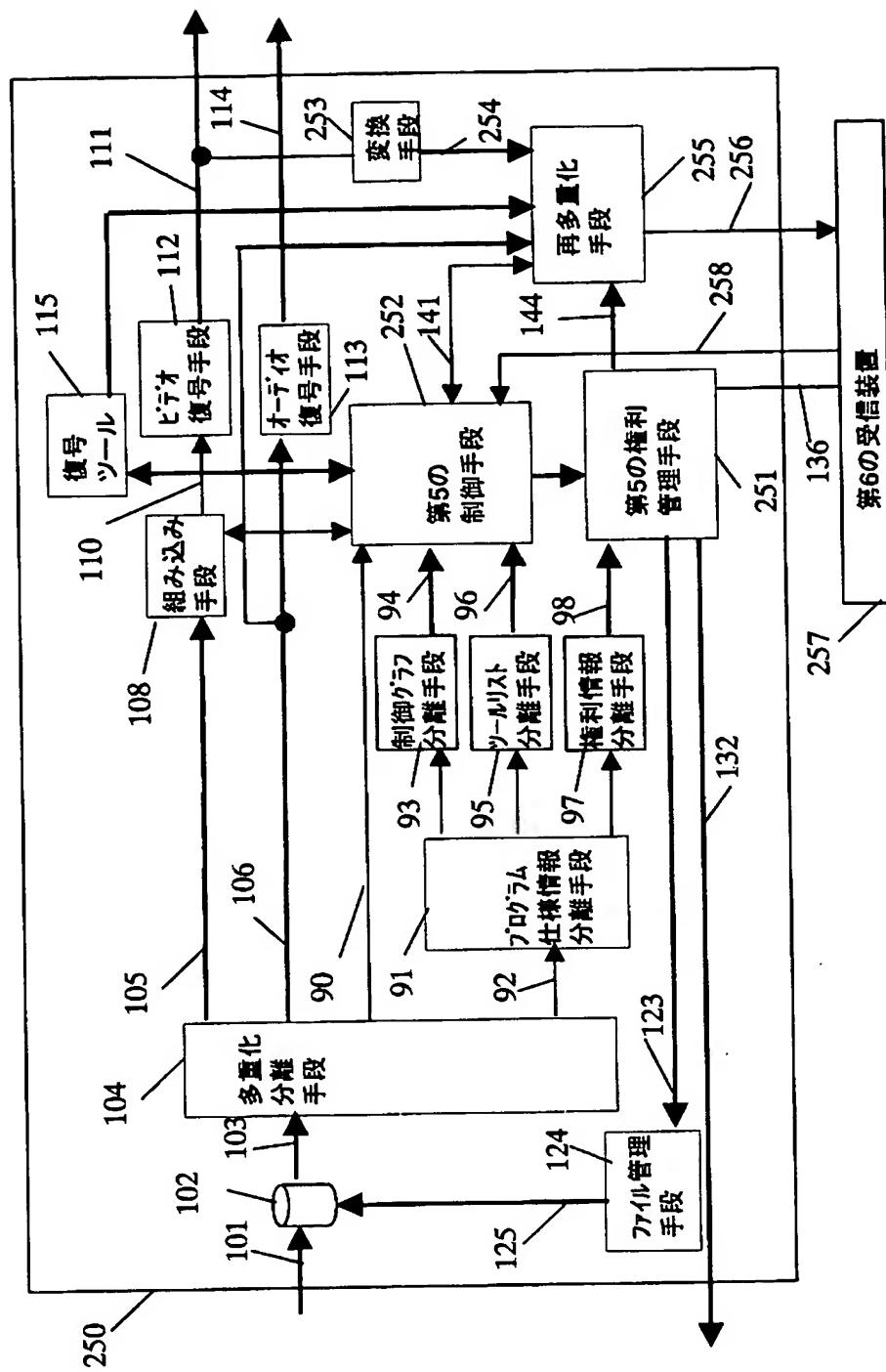
【図 8】



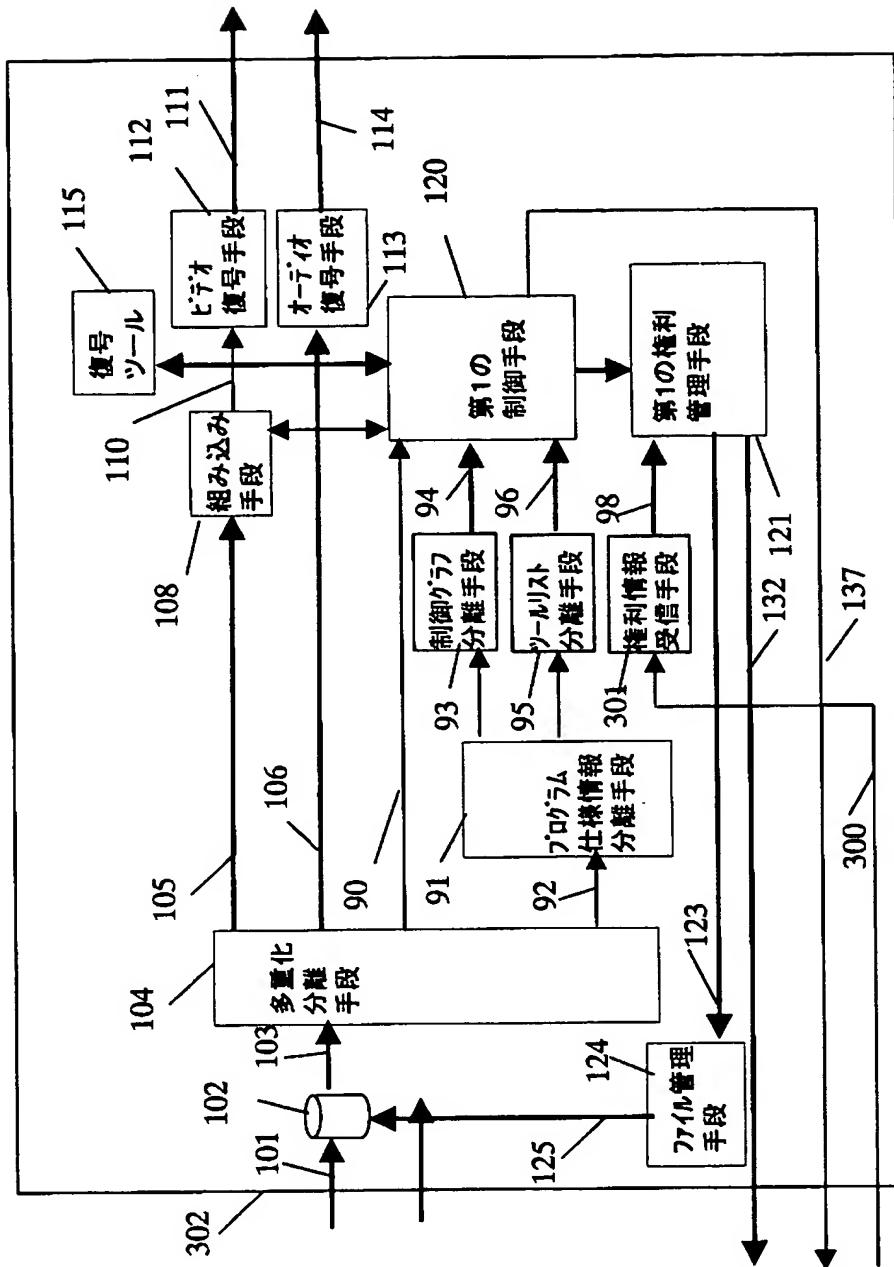
【図9】



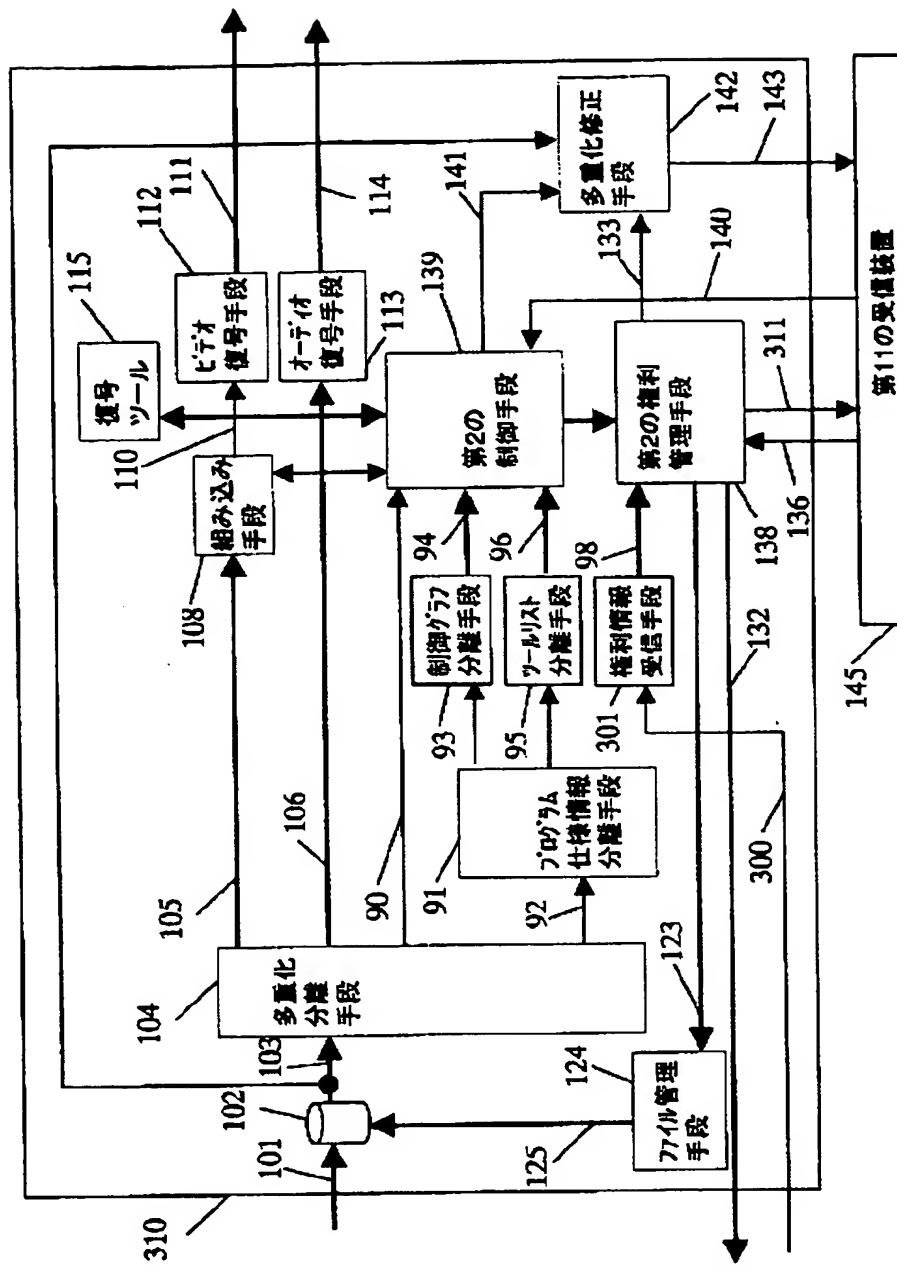
【図10】



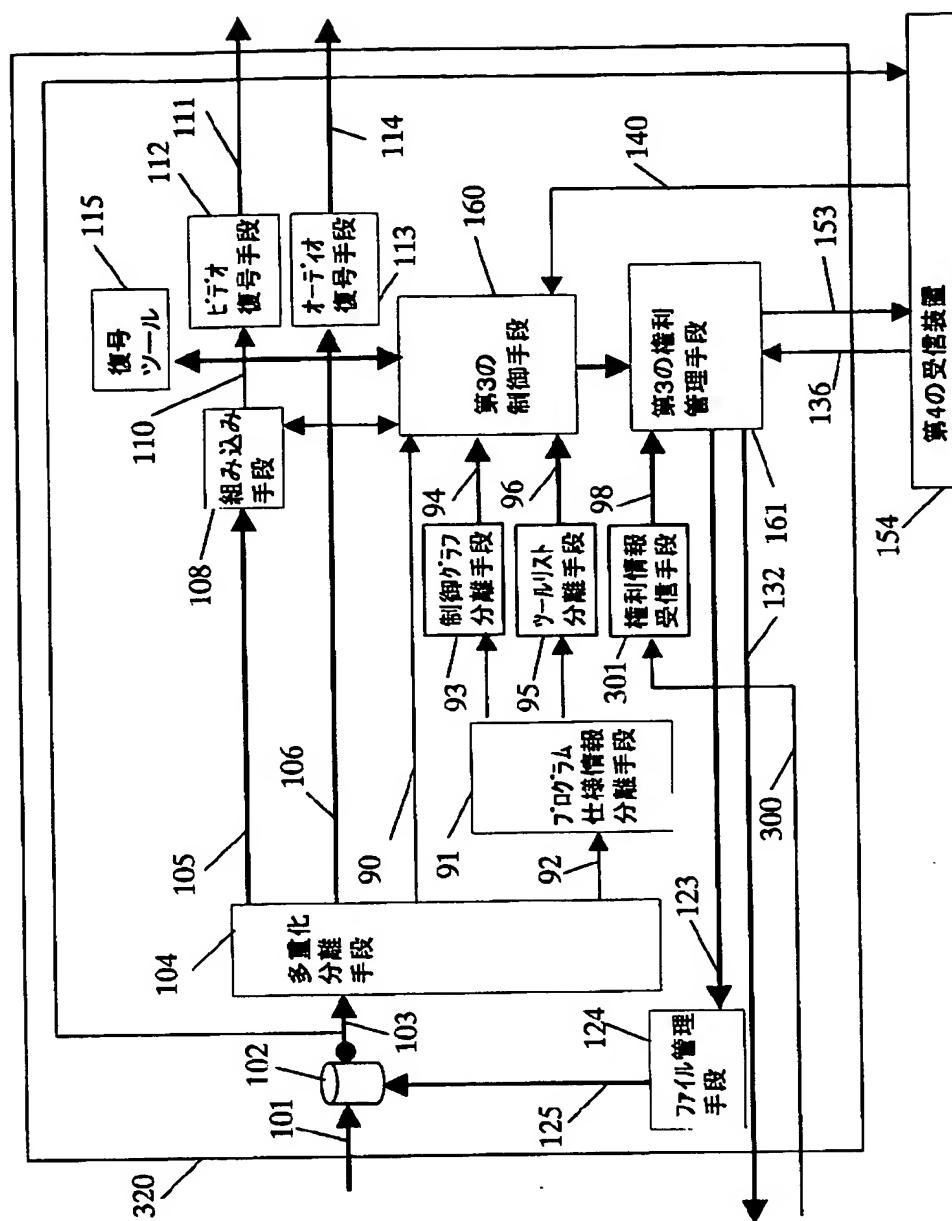
【図11】



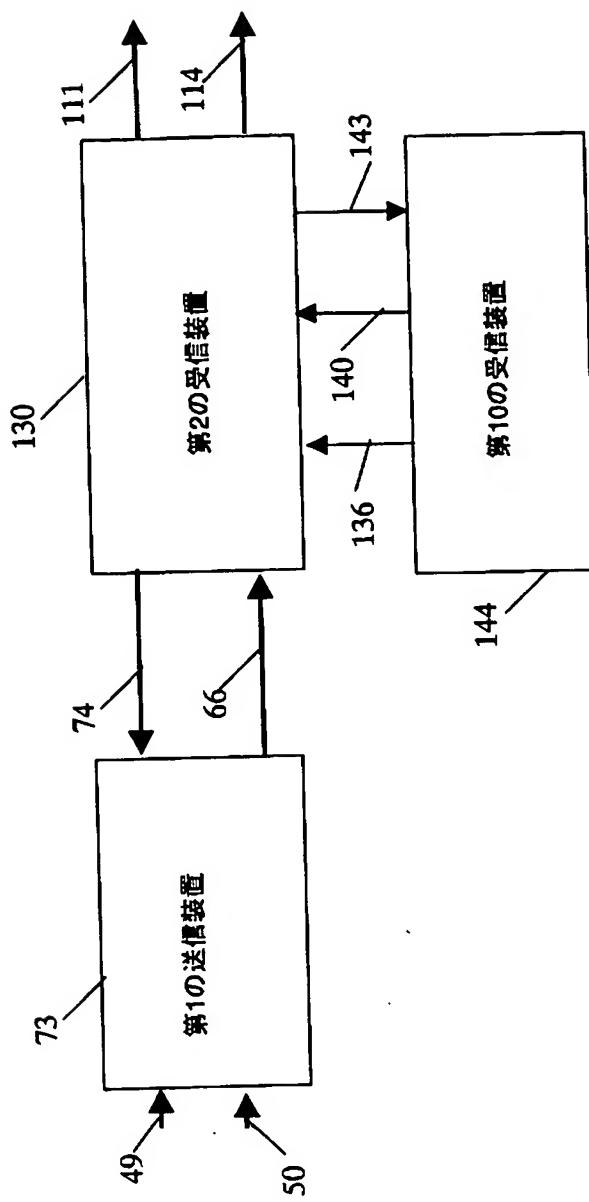
【図12】



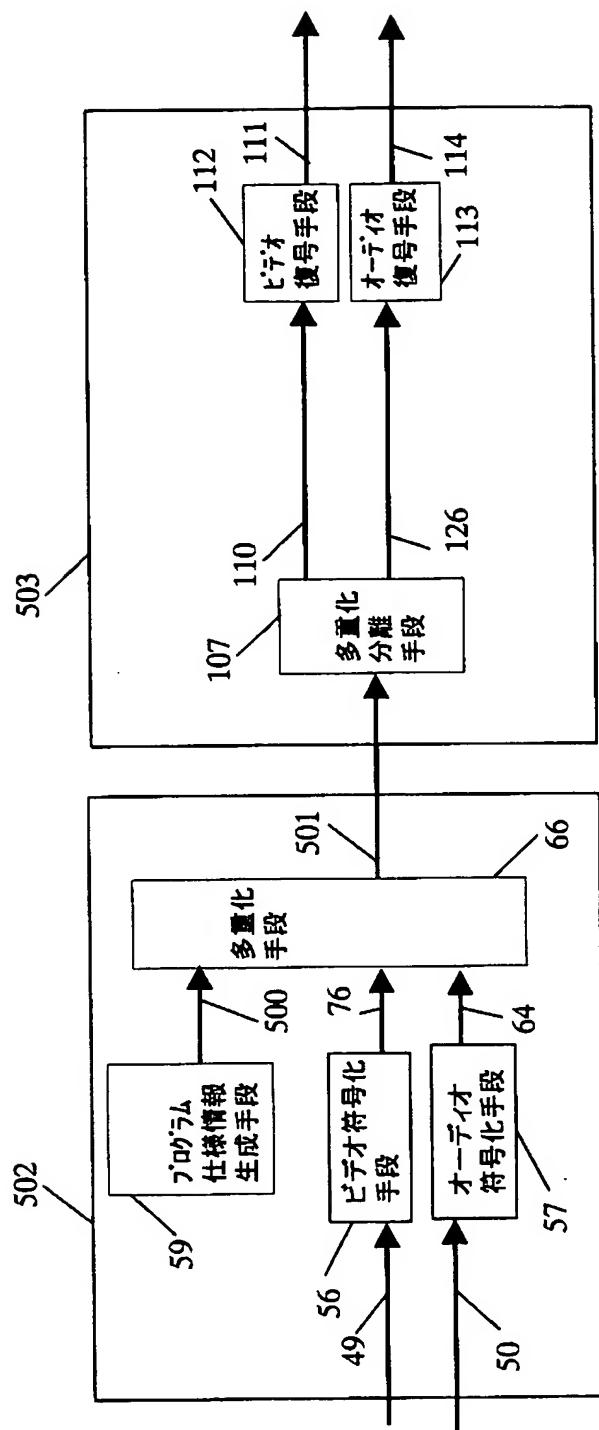
【図13】



【図14】



【図15】



【書類名】 要約書

【要約】

【課題】 暗号化の仕組みを破られた場合に、暗号化の仕組みを更新する送受信装置を提供すること。

【解決手段】 暗号化データの復号ツールのツールIDを取得、存在の確認とツールの取得、更新を行うとともに、上記暗号化データに付随する権利情報に基づいて上記暗号化データの処理と転送を行う。

【選択図】 図1

出願人履歴情報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社